Configuring a Converged User with the "Collaboration Pack for CS 1000" using Avaya Aura® Midsize Enterprise Solution Release 6.2 and Avaya Communication Server 1000 Release 7.5 – Issue 1.0

Abstract

This Application Note describes the detailed procedures for configuring a Converged User with the "Collaboration Pack for CS 1000". This solution consists of the Avaya Communication Server 1000 Release 7.5 and the Avaya Aura® Midsize Enterprise solution Release 6.2. In the sample configuration described herein, a Converged User is defined as a user having a Communication Server 1000 client and a Collaboration Pack client sharing the same Directory Number such that simultaneous ring (SIMRING), a single Avaya CallPilot voicemail box and aggregated Presence are enabled for the user. The steps documented in this Application Note focus on how these attributes are configured across the solution.

Avaya Aura® Midsize Enterprise solution is virtualized to a single server which includes a flexible SIP-enabled communications platform, messaging, conferencing, centralized management and administration tools, and an application development interface. Each capability operates the same as when running on its own server. Communication Server 1000 is a telephony application server used here to provide the Converged User capability. A narrow set of client endpoints as well as capabilities of the Avaya Aura® solution were tested in this sample configuration.

Table of Contents:

1. Introduction 4
2. General Test Approach and Test Results 5
   2.1. Interoperability Compliance Testing 5
   2.2. Test Results and Observations 6
3. Reference Configuration 7
   3.1 Avaya Aura® Midsize Enterprise Solution Components 7
3. Equipment and Software Validated 9
4. Configure Avaya Communication Server 1000E 10
   4.1. Enable UCM Services in SMGR 10
   4.2. Confirm Node and IP Addresses 12
   4.3. Confirm Virtual D-Channel, Routes and Trunks 14
      4.3.1. Confirm Virtual D-Channel Configuration 14
      4.3.2. Confirm Routes and Trunks Configuration 14
   4.4. Configure SIP Trunk to Avaya Aura® Session Manager 16
   4.5. Configure ESN for Route List Index and Digit Manipulation 19
   4.6. Configure Avaya Communication Server 1000 Presence Services 23
      4.6.1. TLS & Certificates section 23
      4.6.2. Change Session Manager Access Point Address: 25
      4.6.3. Verify Communication Server 1000 UCM Security Certificates: 27
      4.6.4. Communication Server 1000 Presence User Agent Configuration: 28
      4.6.5. Configure Presence Publisher to Session Manager 31
      4.6.6. Configure Presence Services for all Communication Server 1000 Users 34
   4.7. Save Configuration 36
5. Configure Avaya Aura® Session Manager 38
   5.1. Verify SIP Domains 39
   5.2. Define Location for Avaya Communication Server 1000 39
   5.3. Configure Adaptation Module 40
   5.4. Define SIP Entities 42
   5.5. Define Entity Links 44
      5.5.1. Entity Links Communication Server 1000 44
      5.5.2. Entity Link for Communication Manager 45
   5.6. Define Routing Policy 46
   5.7. Define Dial Pattern 47
6. Configure Avaya Aura® Communication Manager 50
   6.1. Verify System Access Codes match 50
   6.2. Verify IP Network Region - Domain 53

6.3. Configure Trunk-to-Trunk Transfers 54
6.4. Administer Signal Group 56
6.5. Administer SIP Trunk Group 57
6.6. Verify Signal Group and Trunk Group are In-Service 58
6.7. Configure Incoming Call Handling for Trunk Group 59
6.8. Verify IP Network Region - Domain 60
6.9. Administer Private Numbering Plan (..... 61
6.10. Administer Public Numbering Plan 62
6.11. Administer Uniform Dial Plan 63
6.12. Administer Route Pattern 64
6.13. Administer ARS Analysis 65
6.14. Administer ARS Digit Conversion 66
7. Avaya Aura® Presence Services Configuration 68
7.1. Verify Configuration of Trusted Hosts 68
7.2. Verify Configuration to support Avaya SIP Endpoints 71
8. Configure CallPilot 73
8.1. Registering CallPilot to the Element Registry 73
8.2. Adding CallPilot certificate to System Manager 74
9. User Management 77
9.1. Create User Identities and Communication Profiles in System Manager 77
Select the Commit & Continue button (not shown) 84
9.2. Synchronize Communication Profiles 84
9.2.1. Communication Server 1000 84
9.2.2. CallPilot 86
9.3. Multiple Message Waiting Indication (MWI) for Collaboration 86
9.4. Personal Call Assistant Configuration (PCA) 88
9.5. Manual Configuration of Avaya SIP Clients 90
9.5.1. Avaya Flare® Communicator on iPad 90
9.5.2. Avaya one-X Mobile SIP for iOS on iPhone 92
10. Verification Steps 95
10.1. Verify Operational Status 95
10.1.1. Verify Avaya Aura® Session Manager Operational Status 95
10.1.2. Verify SIP Entity Link Status 96
10.1.3. Verify Registrations of SIP Endpoints 96
11. Conclusion 98
12. Additional References 99
13. Change History 100

1. Introduction

This Application Note describes the procedures for configuring the "Collaboration Pack for CS 1000" with Avaya Aura® Mid Size Enterprise solution Release 6.2 and Avaya Communication Server 1000 Release 7.5.

"Collaboration Pack for CS 1000" offer is based on Avaya Aura® Midsize Enterprise Release 6.2 and is used to accelerate the introduction of new collaboration clients to the Communication Server 1000 installed base. In this initial offer the collaboration clients tested are Avaya SIP clients Flare Communicator for iPad and one-X Mobile (SIP) for iOS. Additional clients and capabilities will be added to "Collaboration Pack for CS 1000" over time.

The notion of a "Converged User" is introduced with the "Collaboration Pack for CS 1000". A Converged User is defined as a user having both a traditional Communication Server 1000 client "twinned" with a collaboration client (such as an Avaya Flare Communicator or one-X Mobile SIP client). These two endpoints are seen by other users to be associated with a single user. They also share a single number for incoming and outgoing calls, single voicemail box via CallPilot and a single aggregated presence.

Avaya Aura ® Midsize Enterprise 6.2 currently supports up to 1,000 users on a single server platform that includes virtualized instances of Avaya Aura® Session Manager, Avaya Aura® System Manager, Avaya Aura® Communication Manager and Avaya Aura® Presence Services. A G430 or G450 gateway is also included as standard with the Avaya Aura® Midsize Enterprise 6.2.

The Avaya Communication Server 1000 R7.5 is used to provide advanced telephony capability to the Converged User via M3900 series digital sets or 1100 / 1200 series IP sets with UNIStim software. PSTN trunks (SIP or ISDN) are also accessed via the Avaya Communication Server 1000 R7.5. Collaboration Pack for CS 1000 is supported via SIP trunks to either CS 1000M or CS 1000E.

CallPilot 5.0 provides voice mail capability to the Converged User, single voicemail box and Message Waiting Indication (MWI). Network Message Service (NMS) capability must be enabled on CallPilot.

Throughout this Application Note the commercial offer, "Collaboration Pack for CS 1000" will be abbreviated and referred as "Collaboration Pack or Collab Pack". Likewise, either an Avaya Flare Communicator on iPad or Avaya one-X Mobile SIP for iOS client will be referred to as "collaboration client or SIP client".

Please complete the following survey to provide feedback on this Application Note.

https://talktous.avaya.com/TakeSurvey.aspx?SurveyID=l44J4n5

2. General Test Approach and Test Results

A reference configuration containing all of the equipment for the Collaboration Pack for CS 1000 was installed at Avaya Test Labs. A number of tests cases were executed to ensure functionality of a Converged User and interoperability between the Communication Server 1000 and Avaya Aura® Mid Size Enterprise solution; aka the Collaboration Pack.

The two clients are "twinned" with one another via the Personal Call Assistant (PCA) feature on the Communication Server 1000. The PCA feature or "PCA call" provides simultaneous ringing (SIMRING) of the two clients in the case of an incoming call to the Communication Server 1000 client. The user can answer on either client, (Communication Server 1000 client or collaboration client on the Collaboration Pack) and the other will stop ringing. In the case of no answer or busy, call redirection will occur as defined for the Communication Server 1000 client – this could include redirection to a single CallPilot voice mailbox. In the case of an outgoing call from the Converged User, in the case of the Avaya SIP client on the Collaboration Pack, the Calling Line Identification (CLID) feature of Communication Manager is used to send the CLID associated with the Communication Server 1000 client to ensure single number identity. For presence aggregation the telephony presence of the Communication Server 1000 client is pushed to the Avaya Aura® Presence Services, which also receives/pushes presence updates for the collaboration client

PSTN calling is achieved via the Communication Server 1000 for all clients. This can be via ISDN or SIP trunks.

2.1. Interoperability Compliance Testing

To verify the interoperability and operation of a Converged User the following features and functionality were covered during the testing:

- Simultaneous ringing for inbound calls
- Single number for CLID on incoming and outgoing calls
- Single voicemail box via CallPilot
- MWI via CallPilot
- Voicemail navigation for inbound and outbound calls via CallPilot
- Aggregation of presence status across devices for a Converged User
- Incoming and outgoing PSTN calls
- Point to point calls (converged user to converged user)
- Multiple call scenarios
- User features such as hold and resume, transfer and conference
- Caller ID presentation during incoming and call transfers
- Proper codec negotiation (G711 and G729)
- E.164 dialing
- Presence status during basic call scenarios
- Call Detail Recording (CDR) on the Communication Sever 1000

The following was not tested with the Collaboration Pack for Communication Server 1000:

- Multiple Communication Server 1000

- High Availability, Geo-redundancy and Branch solutions
- 2,400 users capacity of the Avaya Mid Size Enterprise Server
- MWI, call transfer and conferencing originating from an Avaya Aura® Flare Communicator client
- Off-net call forwarding and mobility (extension to cellular)
- PRI trunking between Communication Server 1000 and Communication Manager
- Presence status with a one-X Mobile SIP client
- ACD agent as a Converged User
- PSTN calls routed thru the Communication Manager
- Avaya one-X Communicator for Communication Manager and Communication Server 1000
- Avaya 96xx phones
- Avaya Aura® Conferencing
- Avaya Aura® Messaging
- Communication Server 1000 features cannot be supported with Communication Manager, e.g. MADN (Multiple Appearance DN), Call Park, Call Pickup, Boss Secretary, etc

2.2. Test Results and Observations

Testing of the Collaboration Pack was completed successfully with the exception of the observations and limitations described below for Converged Users. These items are being addressed and updates will be provided as fixes are made available.
:

- Call transfers which are initiated from an Avaya SIP client (in the reference configuration this was the one-X Mobile client) to a Communication Server 1000 client result in no talk path
- Presence status for Avaya Flare Communicator on iPad as a Converged User does not get updated (from “busy” to “unknown”) upon termination of the call from a Communication Server 1000 client (the presence is updated if a call is attempted or answered from the client)
- Incorrect Calling Party Name and Number on transferred and conference calls: there are a number of different scenarios involving transferred and conference calls where the call display is not properly updated to reflect the true connected party on calls that are either transferred or involved in a conference call. E.g. after the call transfer was completed the tandemed call thru the Communication Server 1000 showed the party that initiated the transfer instead of the actual connected party

3. Reference Configuration

The reference configuration described throughout the Application Note is shown in **Figure 1**.

Figure 1: Reference Configuration

3.1 Avaya Aura® Midsize Enterprise Solution Components

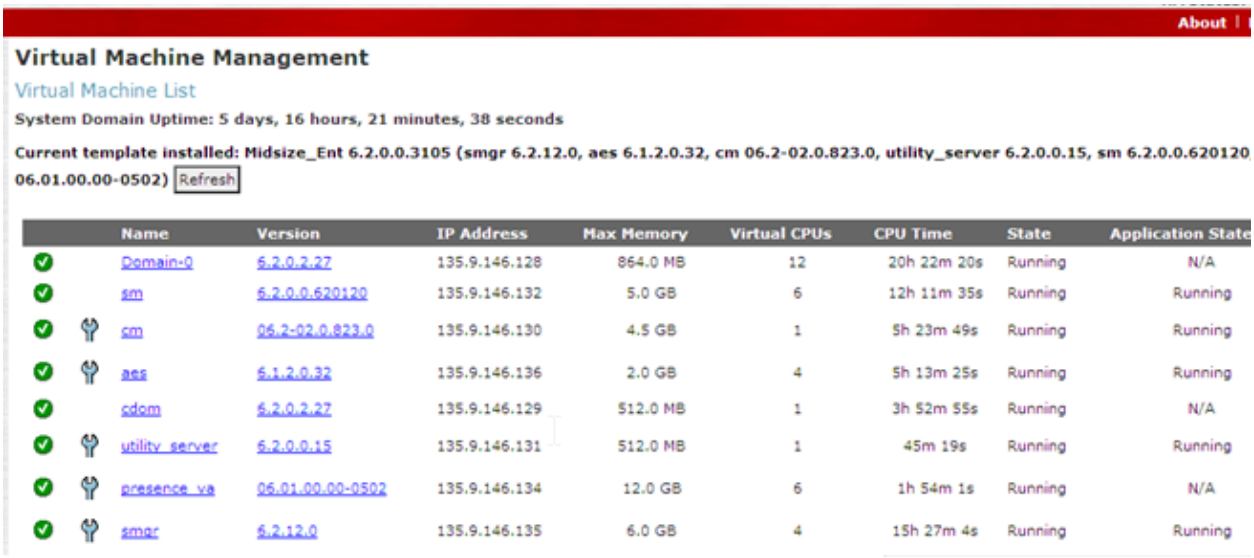
Avaya Aura® Solution for Midsize Enterprise Release 6.2 Template delivers the following applications as virtual machines running on System Platform 6.2:

- Communication Manager 6.2
- Communication Manager Messaging 6.2
- Session Manager 6.2
- System Manager 6.2
- Presence Services 6.1
- Utility Services 6.2
- Application Enablement Services 6.1.2

This Application Note will not cover the software installation of System Platform and the loading of the Midsize Enterprise Template. For more information and step by step instructions on the software installation of System Platform, the Midsize Enterprise Template and initial

configuration for Session Manager, Communication Manager and Presence Server see **Reference [1] thru [3] in Section 12**.

The screenshot shows the list of the applications installed and running on the server, as seen from the Virtual Machine Management screen in System Platform.



Note that Application Enablement and Communication Manager Messaging are installed as part of the Midsize Enterprise Template, but since this application is not being used during this testing, the configuration of this service is not covered in this Application Note.

The other Avaya components used during this testing are:

- Avaya G430 Media Gateway
- Avaya Flare Communicator on iPad
- Avaya one-X® Communicator Mobile SIP for iOS on iPhone and iPod
- Avaya CallPilot 202i
- Avaya Communication Server 1000 IP and digital telephones

SIP trunks will be created between the Session Manager on the Collaboration Pack and Communication Server 1000 to carry outbound and inbound traffic for the collaboration clients. Calls destined to the PSTN from collaboration clients will be routed to the Communication Server 1000 via Session Manager.

Outbound calls to the PSTN originating from the collaboration clients will be first processed by Collaboration Pack for outbound feature treatment such as automatic route selection and class of service restrictions.

Note: The Avaya G430 Media Gateway configuration will not be covered in this App Note. Please refer to **Reference [4] in Section 12** for details.

3. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya Communication Server 1000E running on CPPM server	Release 7.5, Q+ Service_Pack_Linux_7.50_17_20120314.ntl
Avaya Aura® Midsize Enterprise (Session Manager, System Manager and Presence)	6.2 Template 3105
Avaya G430	FW 31.22.0
CallPilot (202i)	5.0 SU11
M3904/5	FW AA94
11xx & 12 xx UNIStim phones	FW 0625C8L
Avaya Flare Communicator on iPad	1.01
Avaya one-X Mobile SIP for iOS	1.04

Table 1: Equipment/Software List

4. Configure Avaya Communication Server 1000E

This section describes the details for configuring Avaya Communication Server 1000E to route calls to the Collaboration Pack as well as provide simultaneous ringing to Avaya Aura® SIP endpoints via Session Manager over a SIP trunk. It also includes details for configuring Presence Services for the Communication Server 1000E. This section does not include information on migrating the Network Routing Service (NRS) to Session Manager. Please see **Reference [5] in Section 12** for these migration steps.

These instructions assume the Communication Server 1000 has been registered a member of the System Manager Security framework. For more information on how to configure System Manager to integrate with the Avaya Unified Communications Management application, see **Reference [7] in Section 12**. **Note: If the UCM Primary Security Server is currently co-resident (with CS 1000 applications) that server will be required to be rebuild as a member server.**

In addition, these instructions also assume the configuration of the CS 1000 Call Server and Signaling Server applications has been completed is configured to support UNIStim (IP) telephones, and Digital telephones. For information on how to administer these functions of Avaya Communication Server 1000E, see **References [6], [7], [8] and [9] in Section 12**.

Using the Avaya Unified Communications Management Element Manager interface, the following administration steps will be described:

- Enable Avaya Unified Communications Management Services in System Manager
- Launch Avaya Unified Communications Management web interface from System Manager
- Confirm Node and IP addresses
- Confirm Virtual Trunks and D-Channel
- Configure SIP Trunk to Session Manager
- Configure ESN – DSC or Special # route prefix for converging
- Configure Presence Service # and Presence Publisher
- Configure Presence Services for all Communication Server 1000 Users
- Save Configuration changes

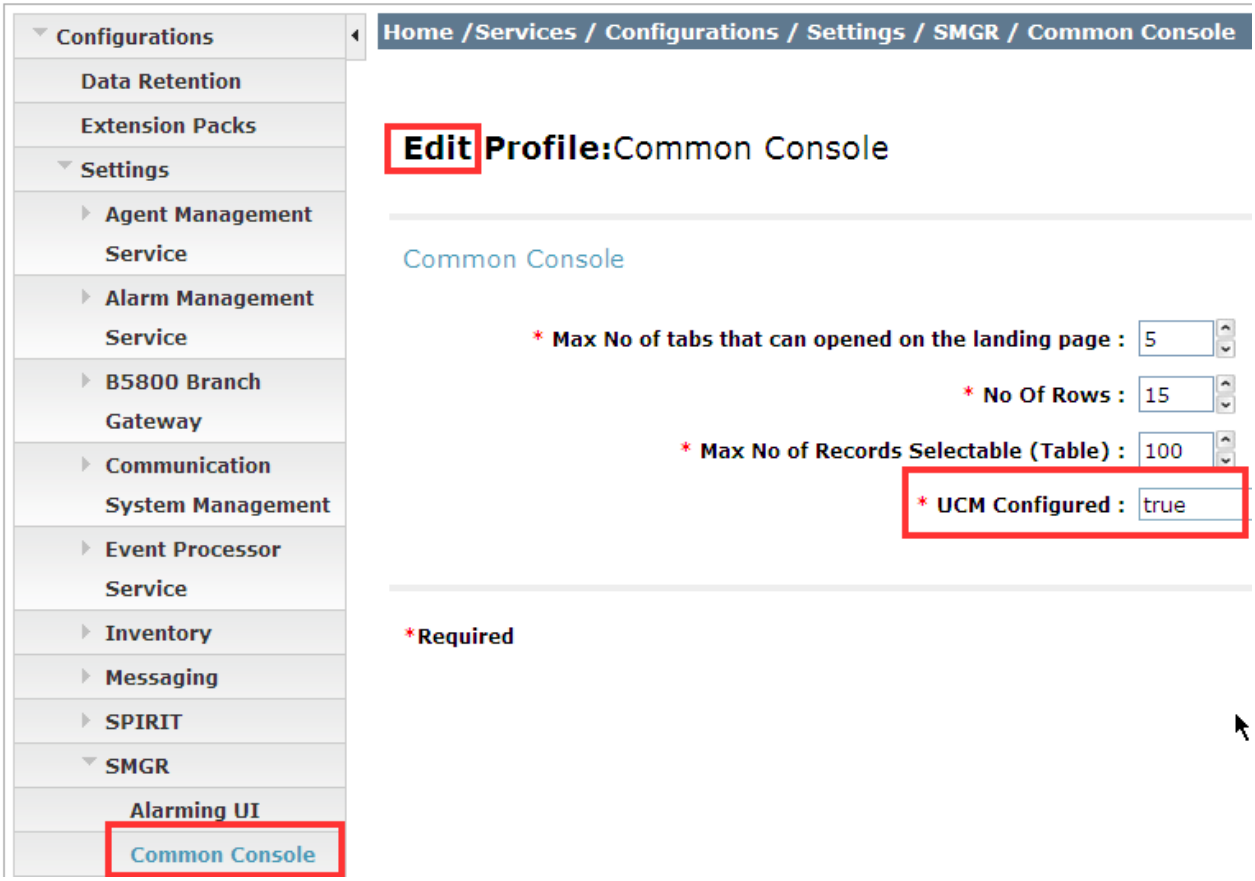
Note: Some administration screens have been abbreviated for clarity.

Access the web based GUI of Avaya Aura® System Manager by using the URL **"http://<ip-address>/SMGR"**, where **<ip-address>** is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

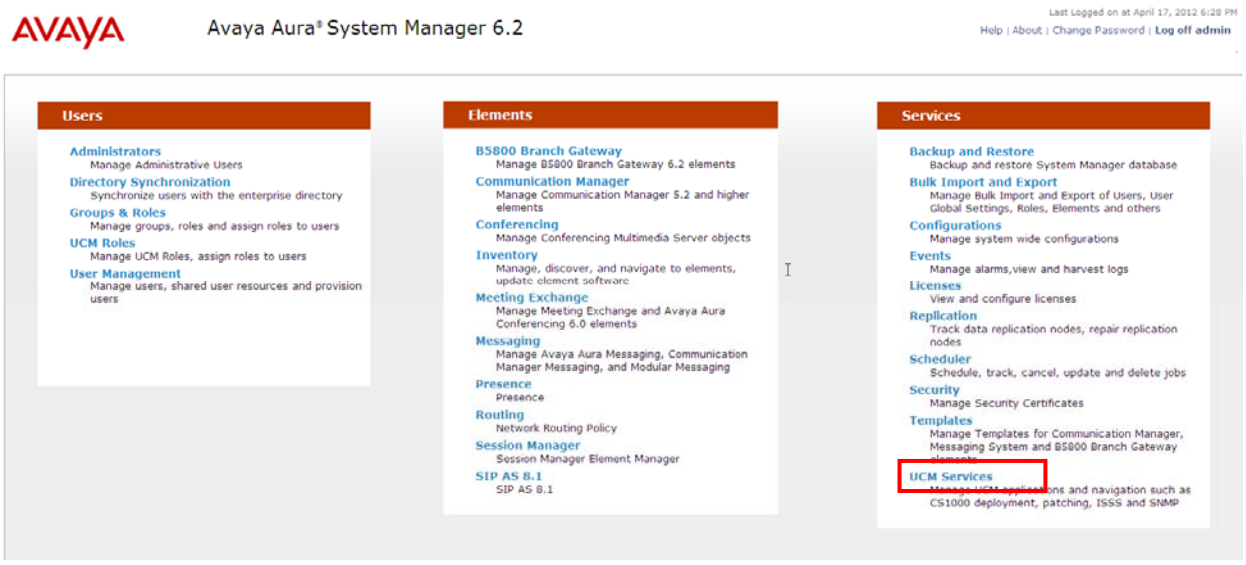
4.1. Enable UCM Services in SMGR

For the UCM Services link to show up in the Home Console of SMGR first enable Common Console and select UCM Configured to **"true".**

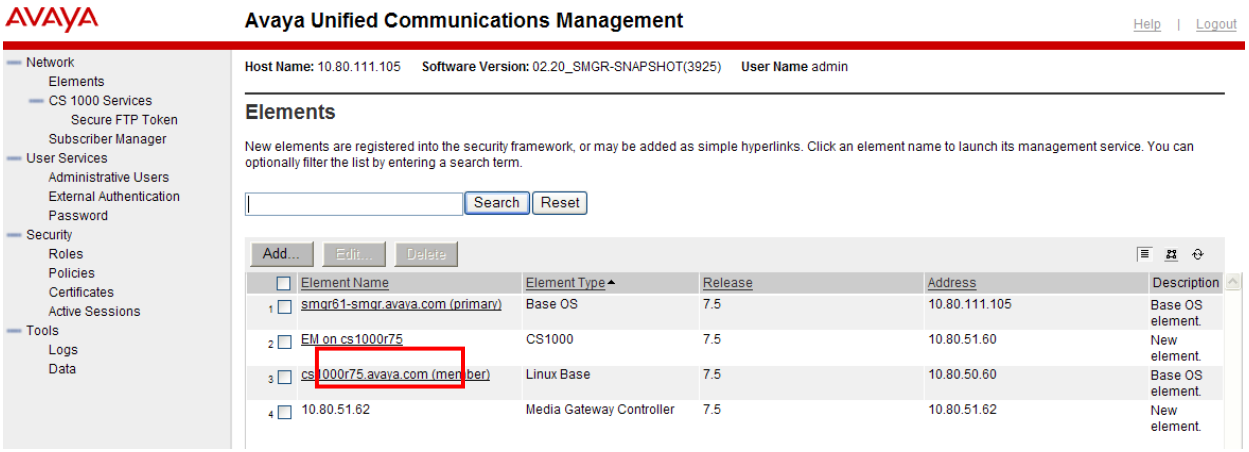
1. **Home /Services / Configurations / Settings / SMGR / Common Console**
2. UCM configured = **"true"**



For the change to take into effect, logout of System Manager and log back-in. Avaya Aura® System Manager Home Page will be displayed. Use the **Services** category on the right side and select **UCM Services** for CS1000 management.



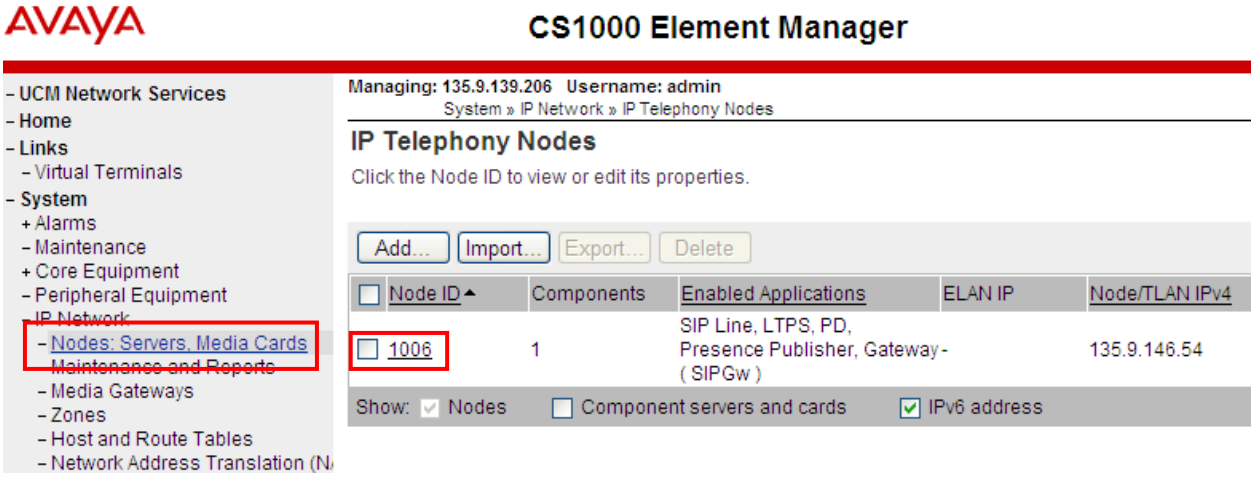
The Avaya Unified Communications Management **Elements** page will open in a new browser window. Select the EM **Element Name** corresponding to **"CS1000"** in the **Element Type** column.



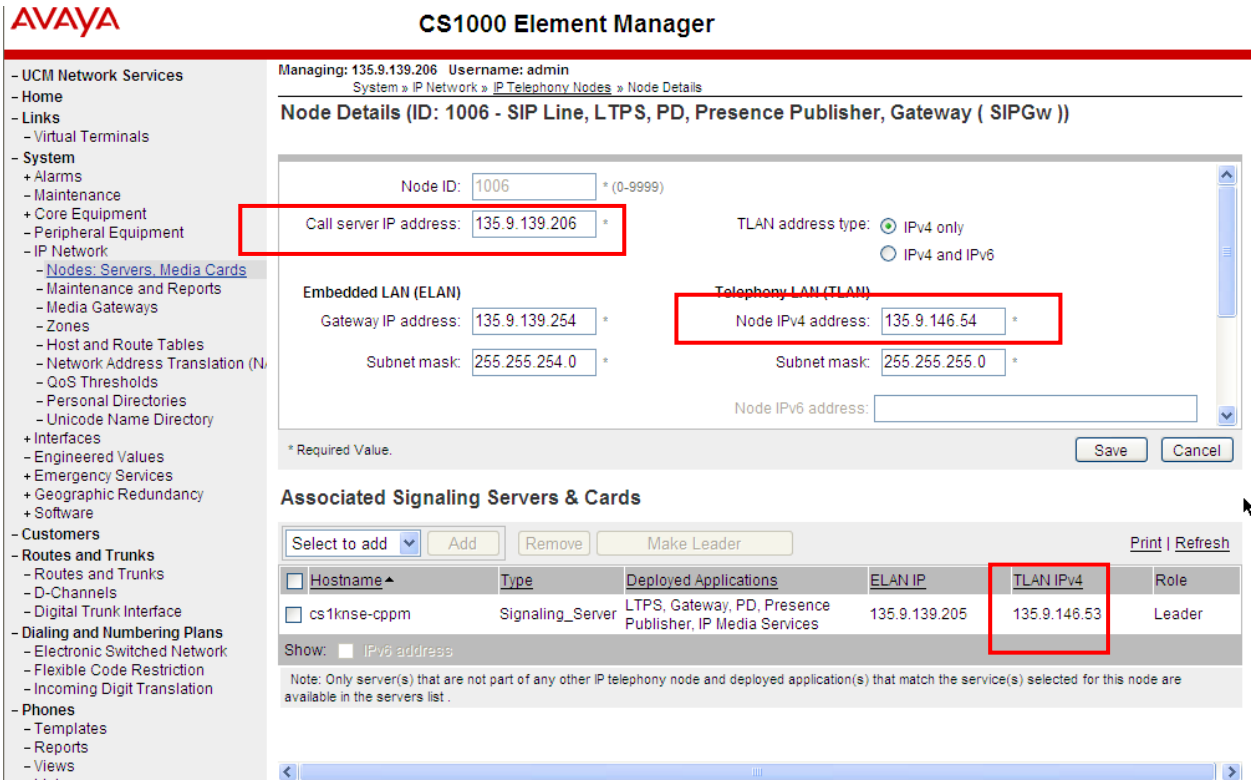
4.2. Confirm Node and IP Addresses

Expand **System → IP Network** on the left panel and select **Nodes: Servers, Media Cards**.

The **IP Telephony Nodes** page is displayed as shown below. Click "**<Node id>**" in the **Node ID** column to view details of the node. In the sample configuration, "**1006**" was used.



The **Node Details** screen is displayed with additional details as shown below. Make a note of the **Node IP address, Call server IP address** and Signaling Server **TLAN IPv4** address fields highlighted below as these values are used to configure other sections.

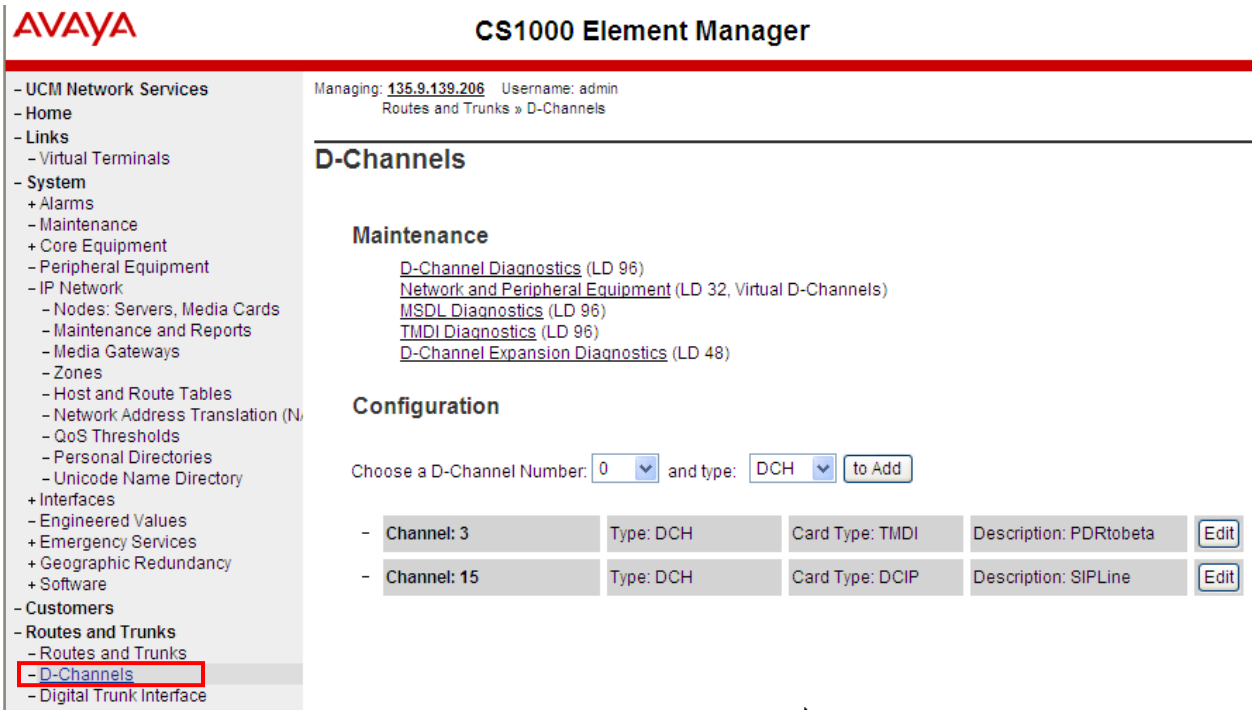


4.3. Confirm Virtual D-Channel, Routes and Trunks

Avaya Communication Server 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server and Session Manager. This section describes the steps to verify that this administration has already been completed.

4.3.1. Confirm Virtual D-Channel Configuration

Expand **Routes and Trunks** on the left navigation panel and select **D-Channels**. The screen below shows all the D-channels administered on the sample configuration.



In the sample configuration, there is a single D-channel assigned to "**Channel: 15"** with "**Card Type: DCIP".** Specifying **"DCIP"** as the type of channel indicates the D-channel is a virtual D-channel.

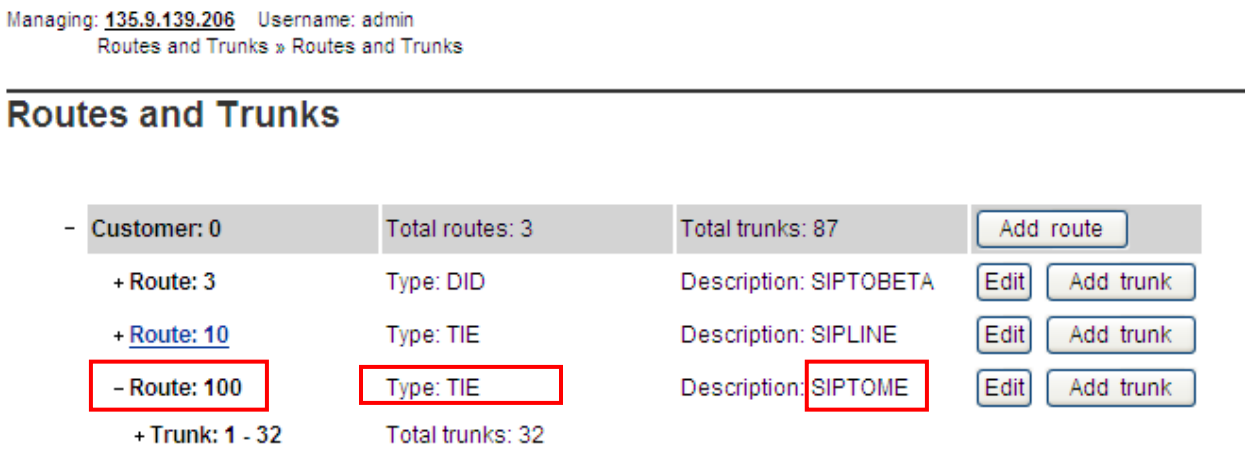
4.3.2. Confirm Routes and Trunks Configuration

In addition to configuring a virtual D-channel, a **Route** and its associated **Trunks** need to be administered.

Ensure this route and trunk member's route to the Session Manager Asset IP address for SIP traffic.

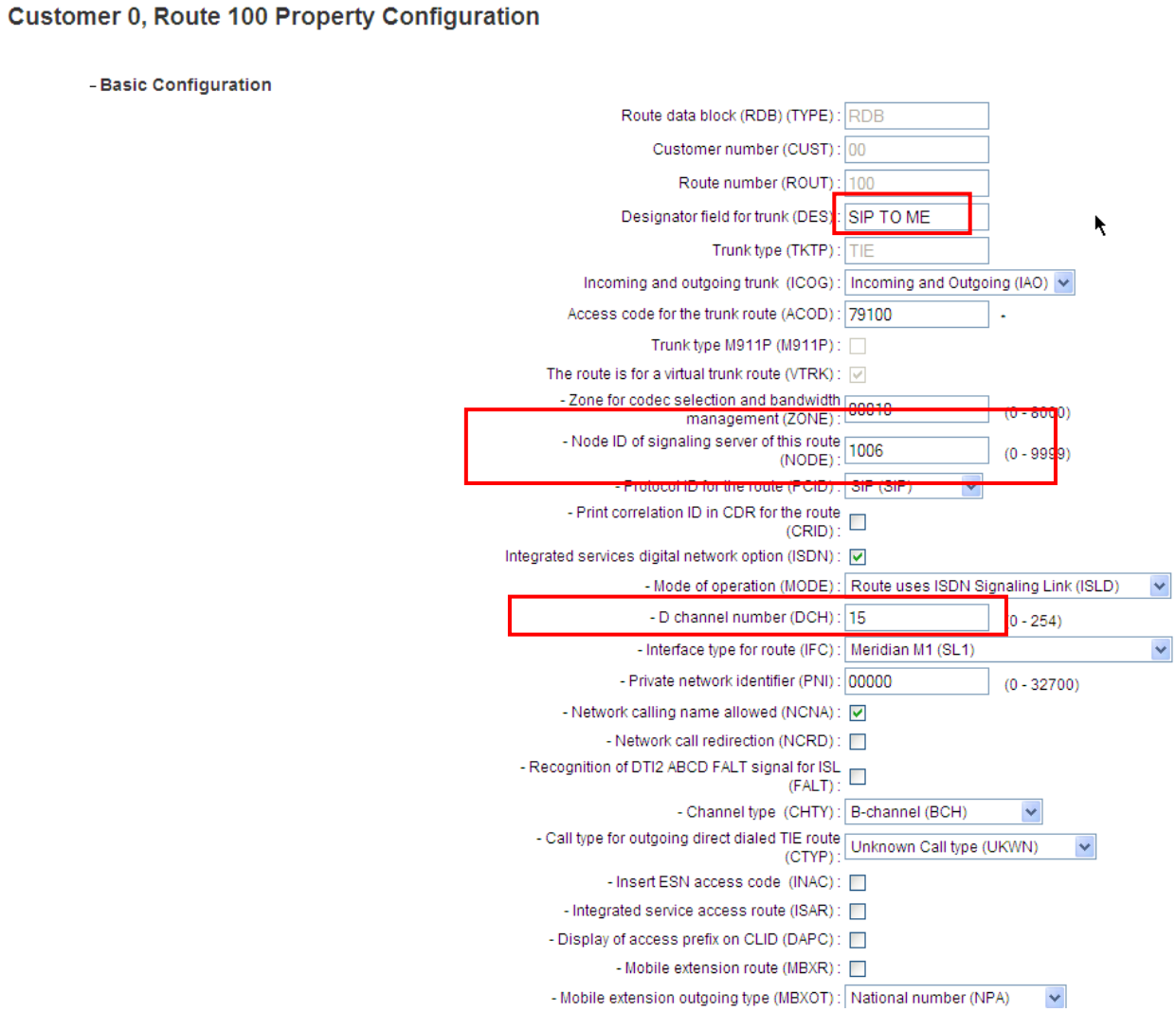
Expand **Routes and Trunks** on the left navigation panel and select **Routes and Trunks** (not shown) to verify a route with enough trunks to handle the expected number of simultaneous calls has been configured.

As shown in the screen below, "**Route 100"** has been configured with 32 trunks which indicate the system can handle 32 simultaneous calls out to Session Manager over SIP.



Select **Edit** to verify the configuration.

The details of the virtual Route defined for sample configuration is shown below. Verify "S**IP (SIP)"** has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** and **D channel number (DCH)** fields match the values identified in the previous section.



4.4. Configure SIP Trunk to Avaya Aura® Session Manager

Expand **System - IP Network - Nodes: Servers, Media Cards**.

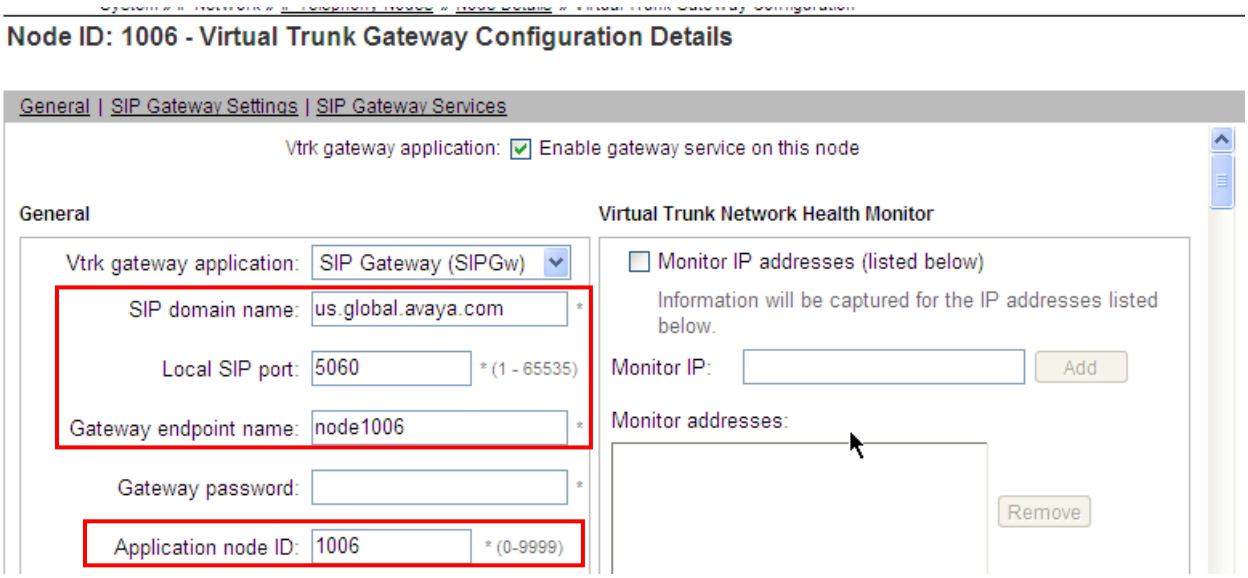
Select "**1006**" in the **Node ID** column (not shown) to edit configuration settings of node.

Using the scroll bar on the right side of the screen, navigate to the **Applications** section on the screen and select the **Gateway (SIPGw)** link (not shown).

On the **Node ID: 1006 - Virtual Trunk Gateway Configuration Details** page, confirm the following values and use default values for remaining fields**.**

- **SIP domain name:** Enter name of domain.
  In the sample configuration,
  "**us.global.avaya.com**" was used.
- **Local SIP port:** Enter "**5060**"
- **Gateway endpoint name:** Enter descriptive name
- **Application node ID:** Enter "**<Node id>**".
  In the sample configuration, "**1006**" was used.

The values defined for the sample configuration are shown below.



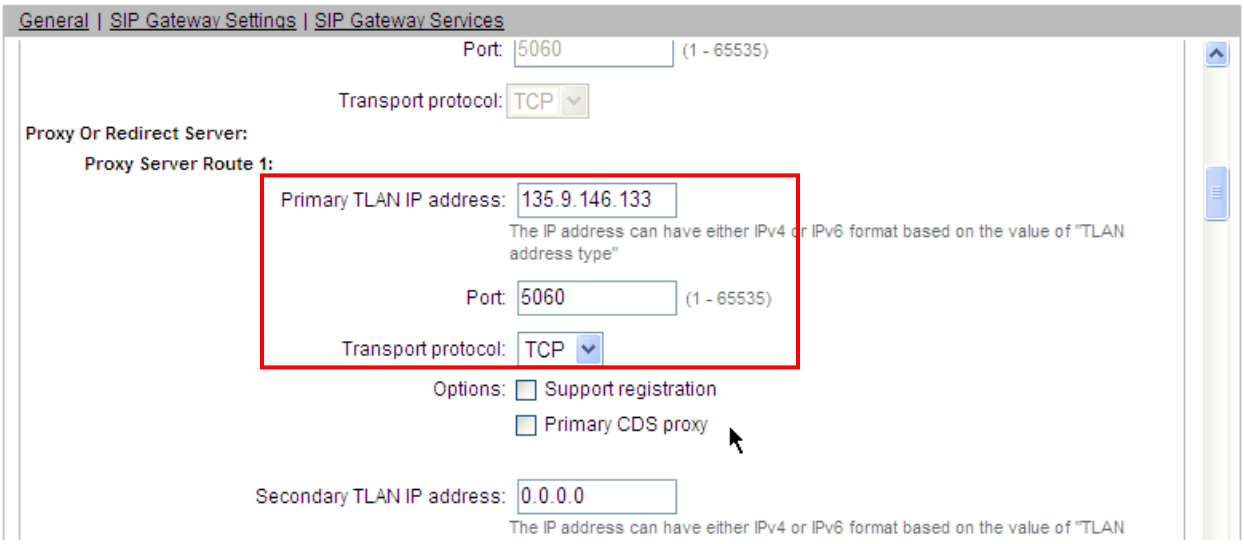
Scroll down to **SIP Gateway Settings - Proxy or Redirect Server**: section of the page.

Under **Proxy Server Route 1:** section, enter the following values and use default values for remaining fields**.**

- **Primary TLAN IP address:** Enter IP address of the Session Manager SIP signaling asset "**135.9.146.133**"
- **Port:** Enter "**5060**"
- **Transport protocol:** Select "**TCP**"

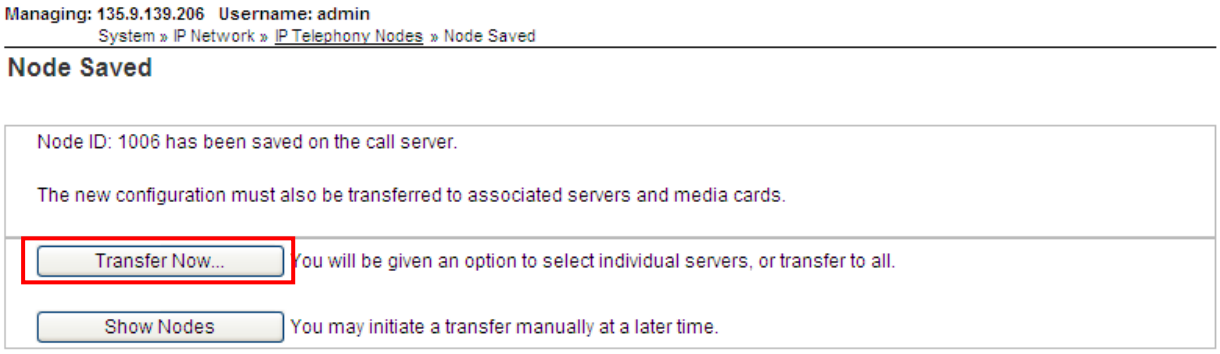
Note: TCP was used for the sample configuration. However, TLS would typically be used in production environments. For more information on configuring the system to use TLS, see **Reference [5]** in **Section 12.**

The values defined for the sample configuration are shown below.

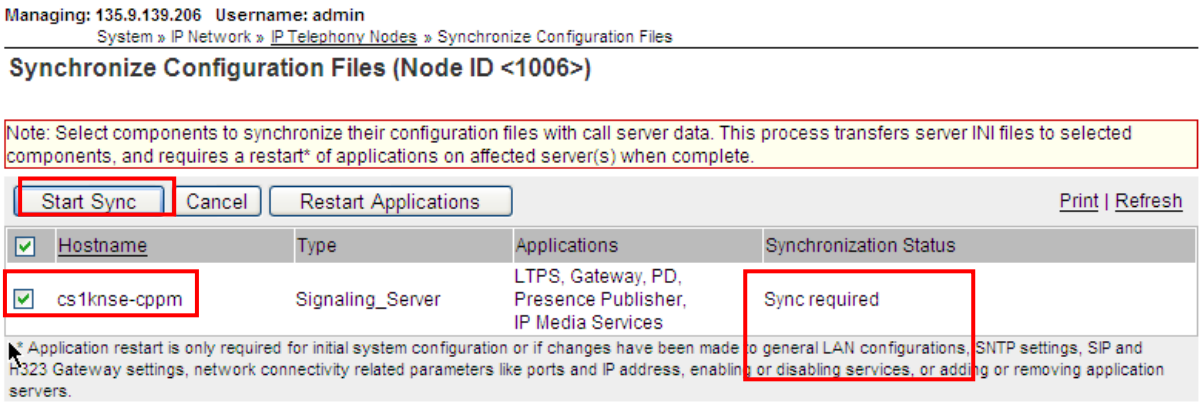


Click **Save** on the **Node Details** screen (not shown).

Select **Transfer Now** on the **Node Saved** page as shown below.



Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.



Enter ☑ associated with the appropriate Call Server and click **Start Sync.** The screen will automatically refresh until the synchronization is finished. The **Synchronization Status** field will update from **Sync required** (as shown) to **Synchronized** (not shown).

After synchronization completes, click **Restart Applications** to use new SIP Gateway settings.

4.5. Configure ESN for Route List Index and Digit Manipulation

This section provides the configuration of the routing used in the sample configuration for routing calls over a SIP Trunk between the Communication Server 1000 on the one side and Session Manager on the Collaboration Pack.

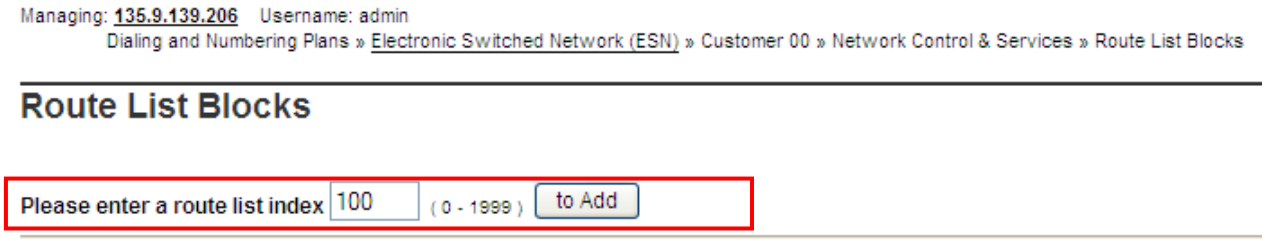
.

Note: The CS1000 Dialing plan and Collaboration Pack routing with adaptations will normalize the dial plan allowing Convergence of User endpoints. The routing rules defined in this section are an example and were used in the reference configuration. Other routing policies may be appropriate for different customer networks.

Step 1: Create Route List Index

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network.**
Select **Route List Block (RLB)**

The **Route List Blocks** screen is displayed. Enter an available route list index number in the **Please enter a route list index** field and click **to Add** as shown below.



Under the **Options** section, select **"<Route id>"** of the route identified in **Section 4.3.2** in the **Route Number** field and use default values for remaining fields as shown below.

Route List Block

General Properties

Number of Alternate Routing Attempts: 5 (1 - 10)
Initial Set: 0 (0 - 64)
Set Minimum Facility Restriction Level : 0
Overlap Length: 0 (0 - 24)
Extended Local Calls:
Route List Index: 100
Entry Number for the Route List: 0 (0 - 63)

Indexes

Time of Day Schedule: 0
Facility Restriction Level: 0 (0 - 7)
Digit Manipulation Index: 100
ISL D-Channel Down Digit Manipulation Index: 0 (0 - 1999)
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route:
Incoming CLID Table: 0 (0 - 1)

Options

Local Termination entry:
Route Number: 100
Skip Conventional Signaling:
Display Originator's Information:
Use Tone Detector:
Conversion to LDN:
Expensive Route:
Strategy on Congestion: Reroute All (RRA)
- QSIG Alternate Routing Causes: QSIG Alternate Routing Cause 1
Preferred Routing: Preferred Route 1
ISDN Drop Back Busy: Drop Back Disabled (DBD)

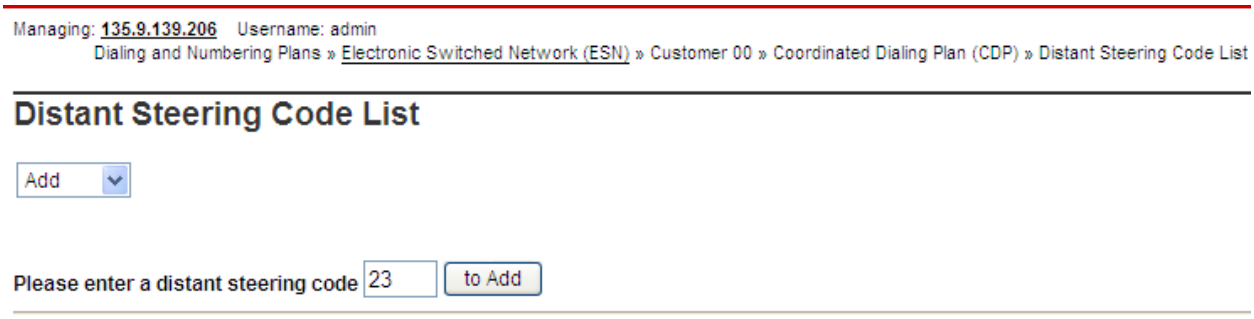
Click **Save** (not shown) to save new Route List Block definition.

Step 2: Create Distant Steering Code

This Digit string will be used as the new unique "Converged Route Prefix" in each CS1000 Users PCA to route calls to the Collaboration Pack via the Session Manager.

Expand **Dialing and Numbering Plans** on the left and select **Electronic Switched Network.** Select **Distant Steering Code (DSC)** under the **Coordinated Dialing Plan (CDP)** section on the **Electronic Switched Network (ESN)** page as shown below.

Select "**Add"** from the drop-down menu and enter the dialed prefix for external calls to be routed over SIP trunk to Session Manager in the **Please enter a distant steering code** field. For the sample configuration, "**23**" was used since SIP endpoints registered to Session Manager were assigned extensions starting with "**23**". Click **to Add** as shown below.

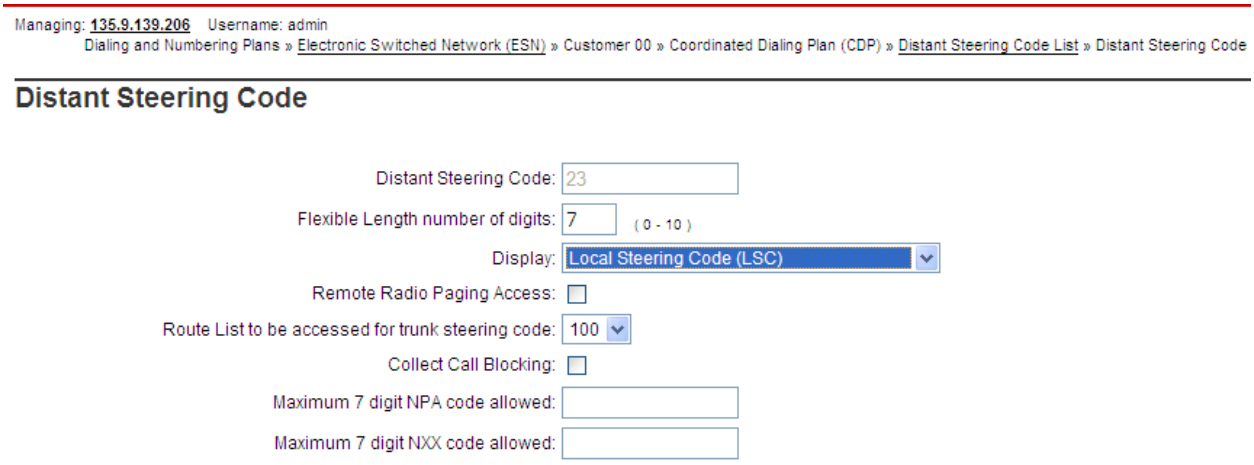


Select the **Flexible Length of number of digits** to be "**7**". This DSC is routed to the Route (RLI) **100** built in the step above.

Enter the following values and use default values for remaining fields.

- **Flexible Length number of digits:** Enter number of digits in dialed numbers
  In the sample configuration, **"7"** was used.
- **Route List to be accessed for trunk steering code:** Select **"<id>"** of Route List Index to be "**100**".

Click **Submit** to save new Distant Steering Code definition.



4.6. Configure Avaya Communication Server 1000 Presence Services

To configure Presence Services with Communication Server 1000 follow **Reference [10], [11] and [12]** in **Section 12.** Please consider the following additional configuration information.

Note : System Manager SP2 is required for this procedure.

4.6.1. TLS & Certificates section

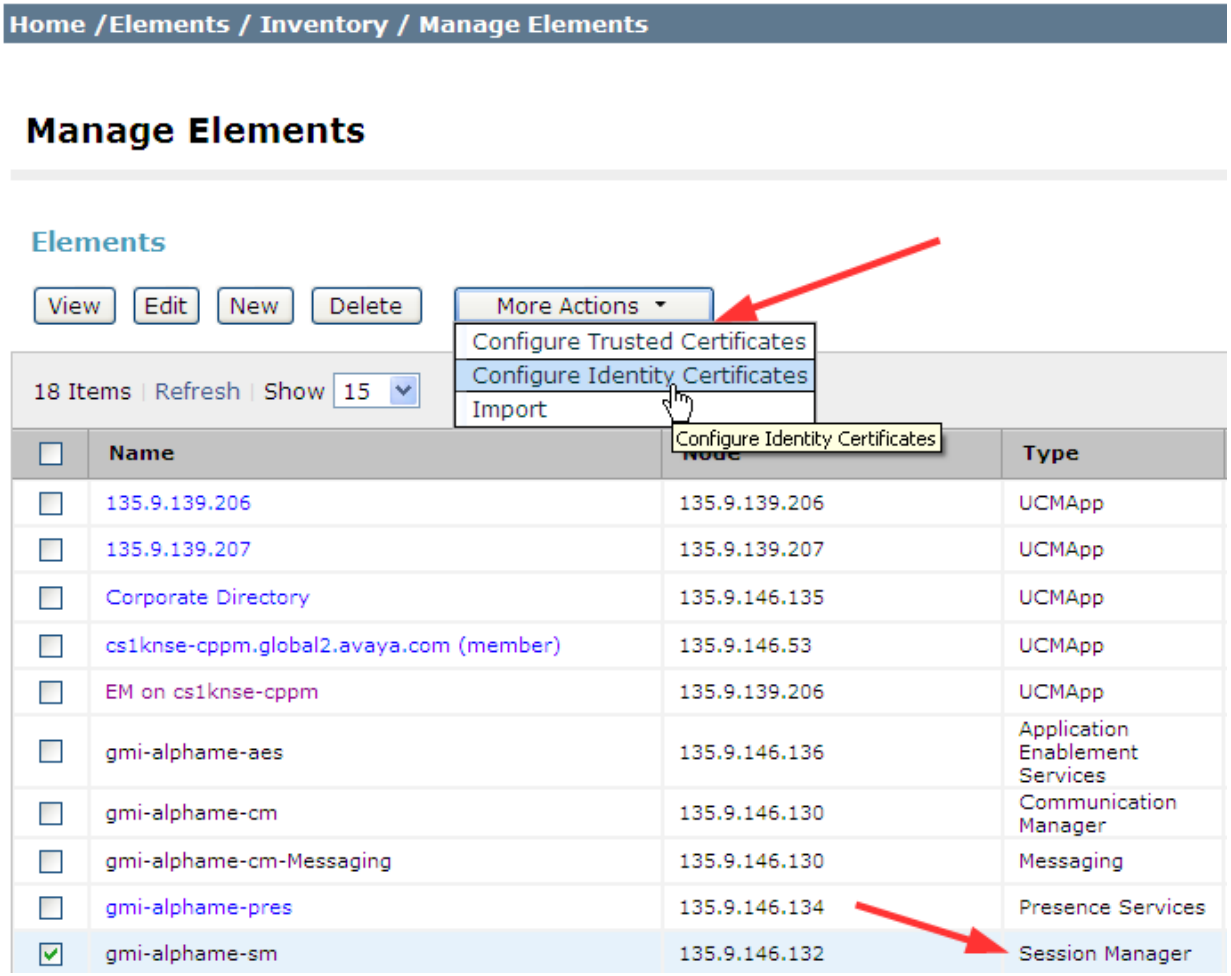
Replacing the Session Manager default certificate:

In the document referenced above in the specific section titled “TLS configuration between CS 1000 and Session Manager”, the Common Name is defined as the “Fully Qualified Domain Name” of the Session Manager.

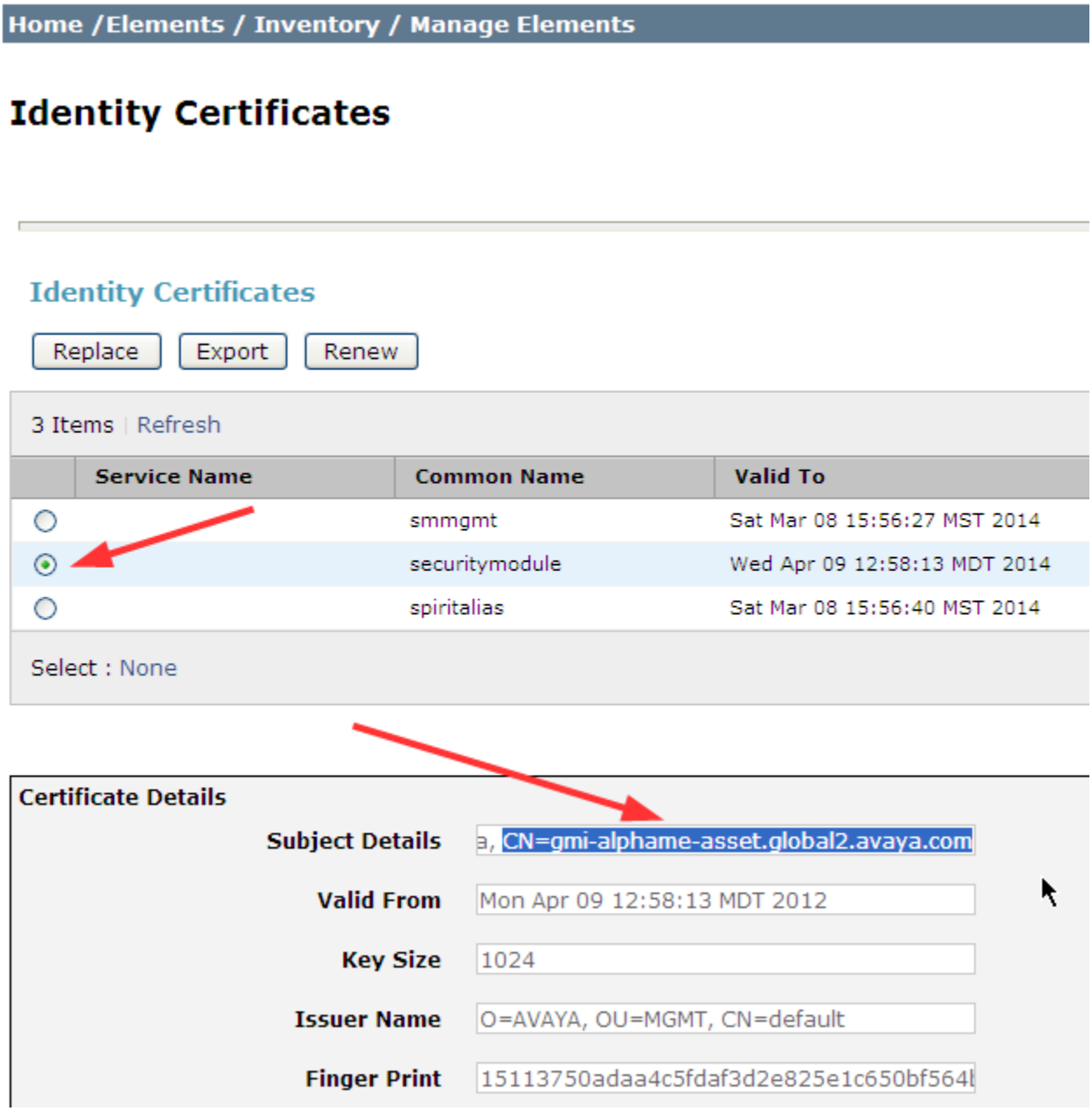
Need to replace the Session Manager default certificate as it uses a hard coded Common Name.
1. In System Manager, navigate to **Elements > Inventory**.
2. In the navigation tree, click **Manage Elements**.
3. In the Entities section, select a Session Manager instance.
4. From the **More Actions** menu, click **Configure Identity Certificates**.
5. Click **security module**, and click the **Replace**.
6. Click **Replace this Certificate with Internal CA Signed Certificate**.
7. Complete the fields for **Common Name**, **Organization Unit**, **Organization**, **Country**, and click **Key Algorithm** and **Key Size**.
8. Verify your data, and click **Commit**.

Common Name is defined as Fully Qualified Domain Name (FQDN) of your Session Manager asset. e.g. C=*US*, O=*Avaya*, CN=***gmi-alphame-asset.global2.avaya.com***

To change the Certificate Common Name Identify navigate from the Home page to:
Inventory - Manage Elements - Select **Session Manager - More Actions - Configure Identity Certificate**



Inventory - Manage Elements - Select **Session Manager – More Actions - Configure Identity Certificate -** Select **Security Module**

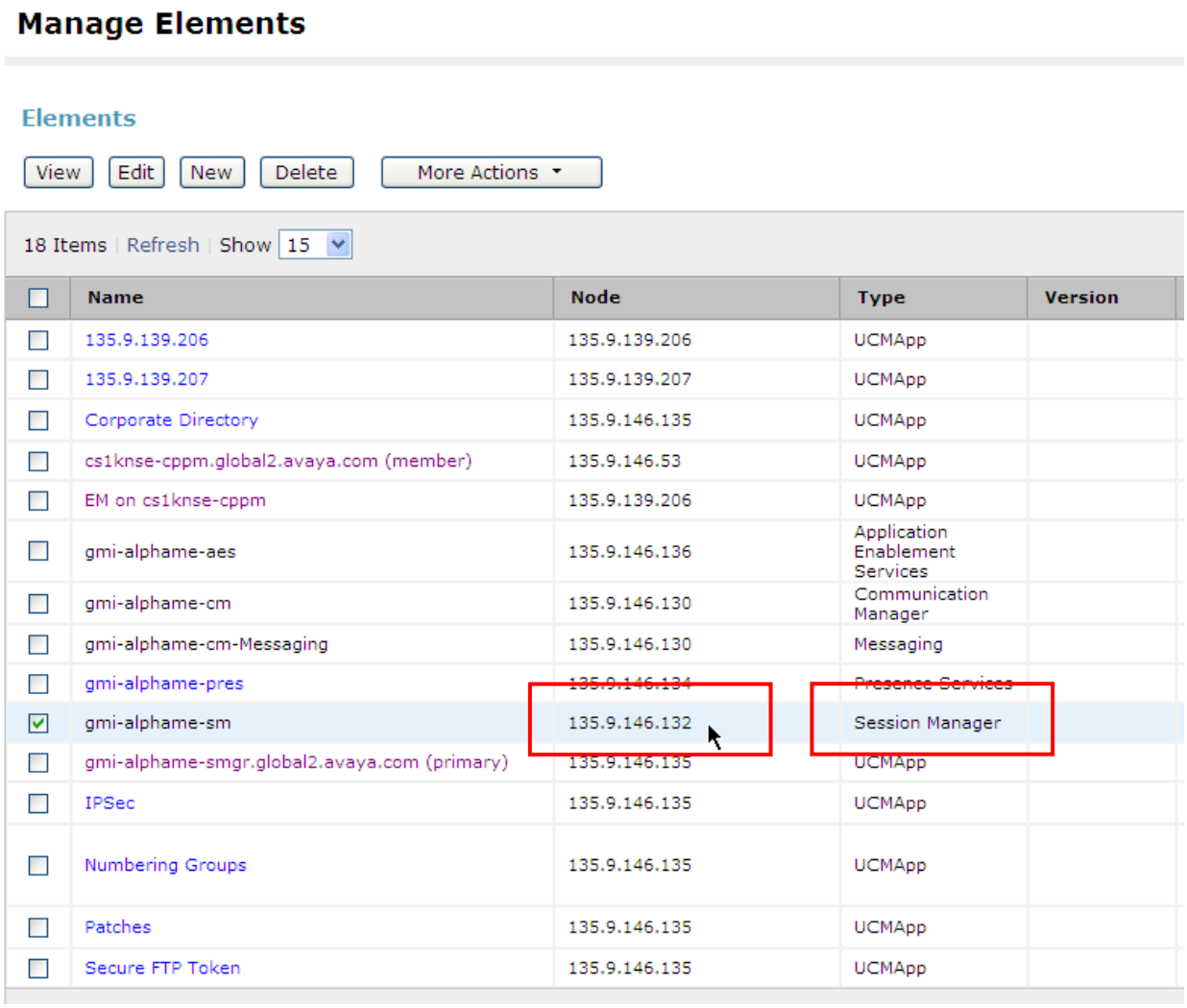


Note as seen in the screen shot above the Certificate Details the Common Name.

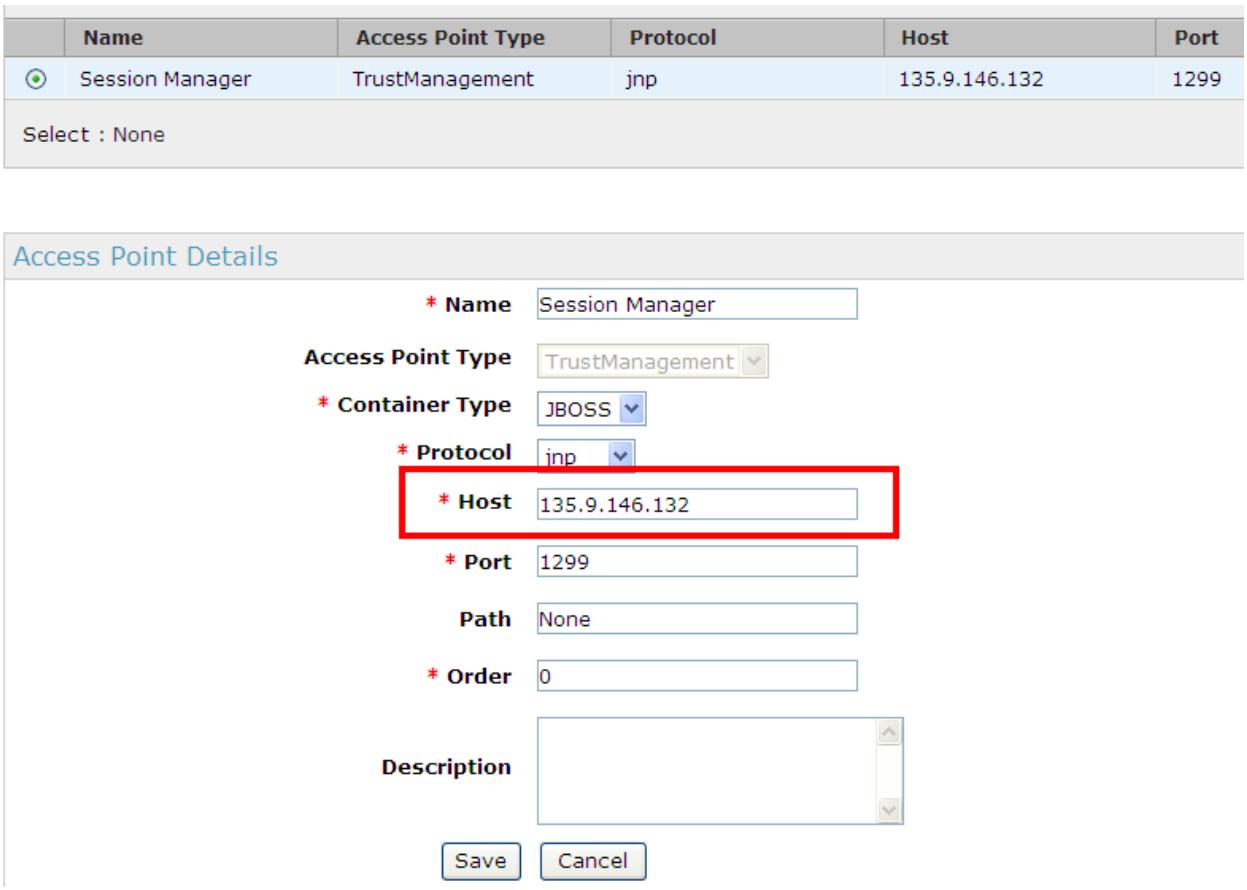
4.6.2. Change Session Manager Access Point Address:

This change is required for the trust management between Session Manager and Communication Server 1000. The Midsize Enterprise template is inserting by default the local host but this must be changed to the Session Manager IP address. To make this change navigate from System Manager Home to:

Inventory → Manage Elements → Select your Session Manager –> Edit -> **Access Point**.



Edit the **Host** from **"localhost"** to the Session Manager IP address. For the reference configuration this is"**135.9.146.132**". Select **Save** then **Commit**.



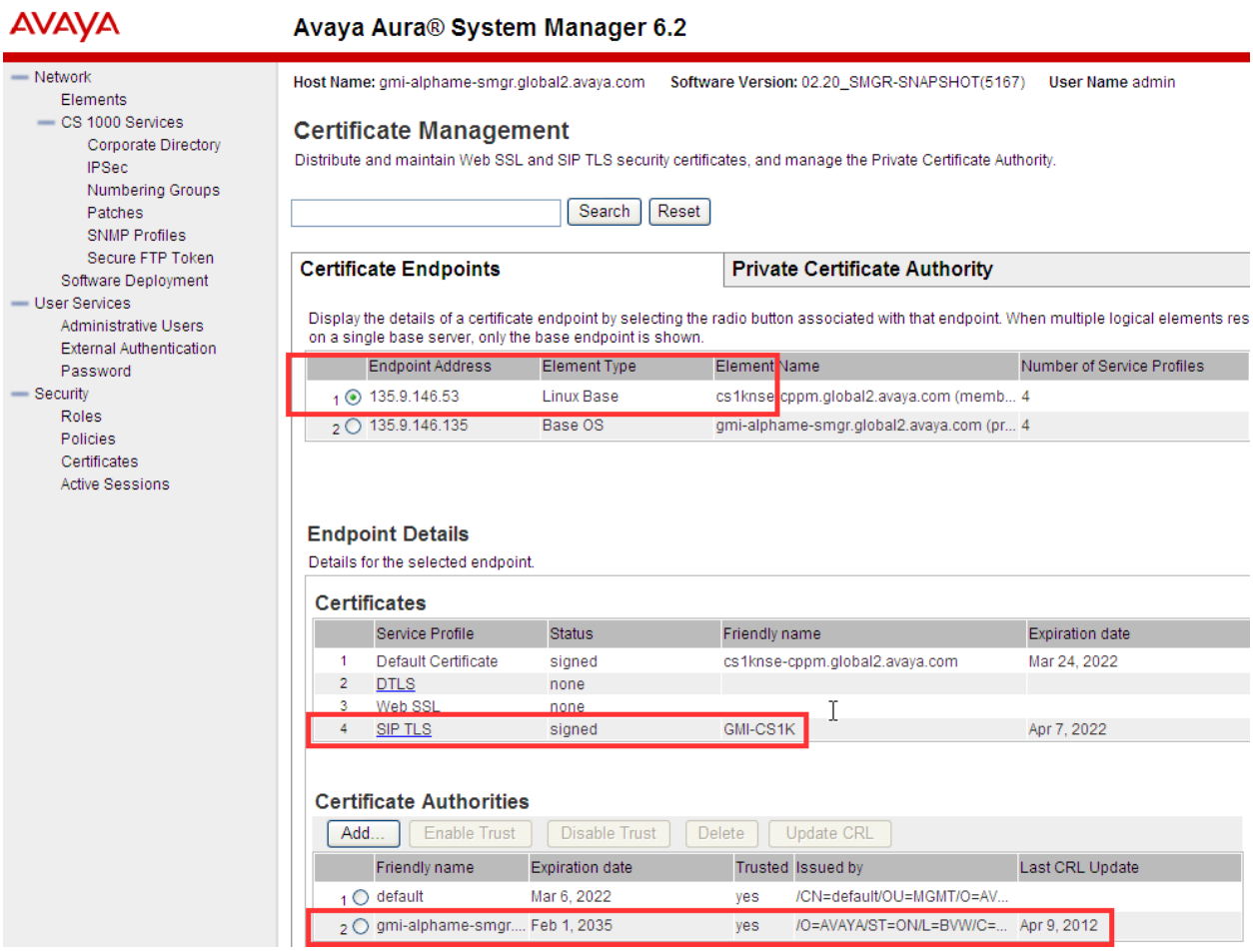
4.6.3. Verify Communication Server 1000 UCM Security Certificates:

For Communication Server 1000 clients to push presence updates to Presence Services they need to communicate over SIP TLS.

Need to confirm the **CS1000 Endpoint Details** – **Certificate** Service Profile – SIP TLS is signed. See the screen shot below.

Navigate to **UCM Services - Security – Certificates**

Select **Linux Base** as element type to view **Endpoint Details.** See screen shot below.



4.6.4. Communication Server 1000 Presence User Agent Configuration:

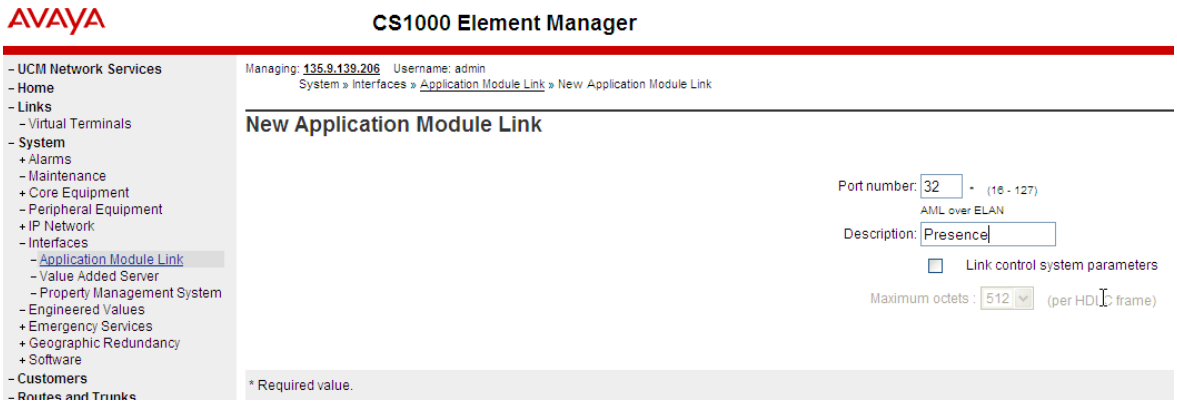
To enable Presence Services on the Communication Server 1000 the following is required to be configured. For detailed steps please refer to **Reference [13]** in **Section 12**.

The following Communication Server 1000 attributes are required to be configured:

- **ELAN AML**
- **VAS ID**
- **ACD DN**
- **CDN**

The **ELAN AML Link** can be configured via LD17 or via System Manager.

Navigate to **UCM Services – Interfaces – Application Module Link.** For the reference configuration, port number "**32**" and Description "**Presence**".



To configure **VAS ID for** AML please follow the following steps in LD17.

Command/Prompt	Command/User Response(s)	Description
REQ	CHG	Change ADAN
TYPE	VAS	
VAS	New	New a VAS
VSID	vasID	The VAS ID number – **e.g. "32"** was used for the reference configuration.
ELAN	ELAN#	ELAN number, should match the one configured in previous step, **e.g. "32"** was used for the reference configuration.

To configure **ACD DN** please follow the following steps in LD23.

Command/Prompt	Command/User Response(s)	Description
REQ	New	New ACD
TYPE	ACD	
CUST	custNum	Customer number
ACDN	Xxxx	An ACD DN to be used when configuring the CDN (PSDN) for Presence. **e.g. "5000"** was used for the reference configuration.

To configure **CDN** please follow the following steps in LD23.

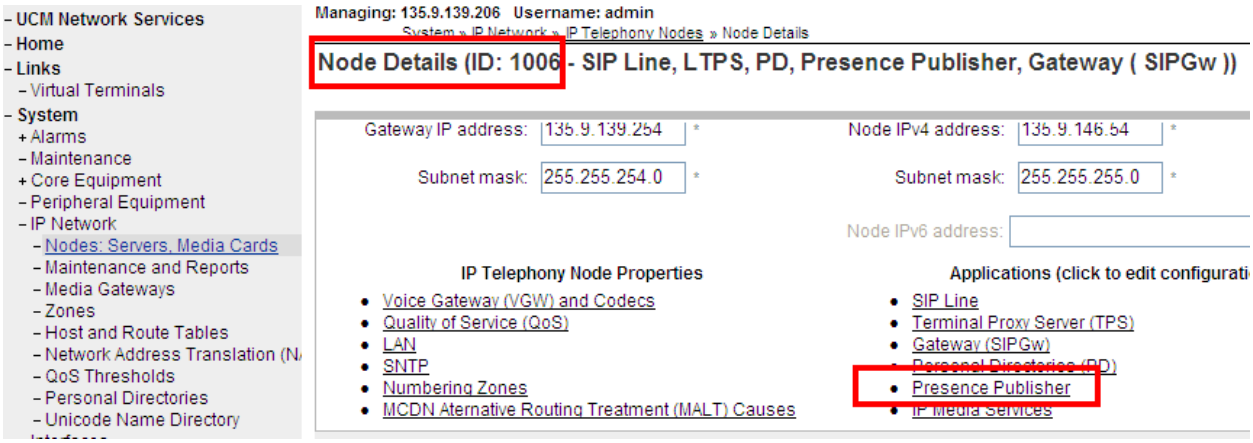
Command/Prompt	Command/User Response(s)	Description
REQ	New	New CDN
TYPE	CDN	
CUST	custNum	Customer number. **e.g. "0"** was used for the reference configuration.
CDN	Xxxx	A number to be used by the Presence Publisher. This CDN is used within the ACD 5000 as the PSDN for each CS1000 user. **e.g. "3000"** was used for the reference configuration. This # must be fit into your Communication Server 1000 overall dialplan.

CDSQ	Yes	This needs to be "**yes"**, so the presence activity is sent to PP.
DFDN	Xxxx	ACD DN **5000** configured in the table as above.

4.6.5. Configure Presence Publisher to Session Manager

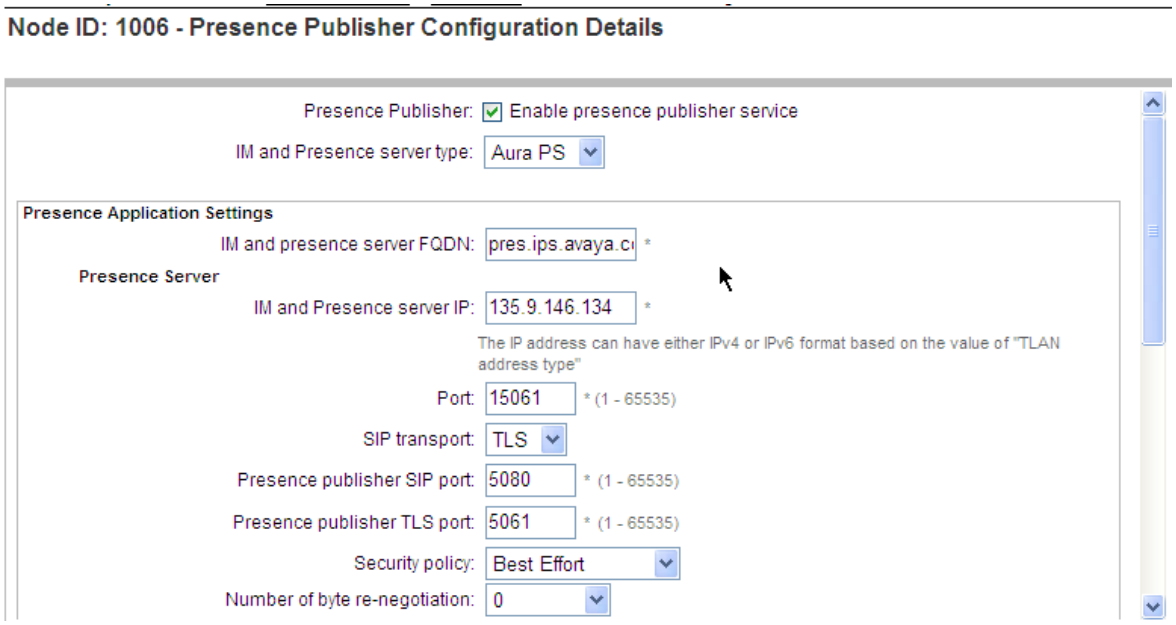
The following configuration is to enable the publishing of Presence updates for Communication Server 1000 endpoints.

Navigate to **UCM Services – EM – IP Network – Nodes: servers, Media Cards-Node 1006** Using the scroll bar on the right side of the screen, navigate to the **Applications** section on the screen and select the **Presence Publisher** link.



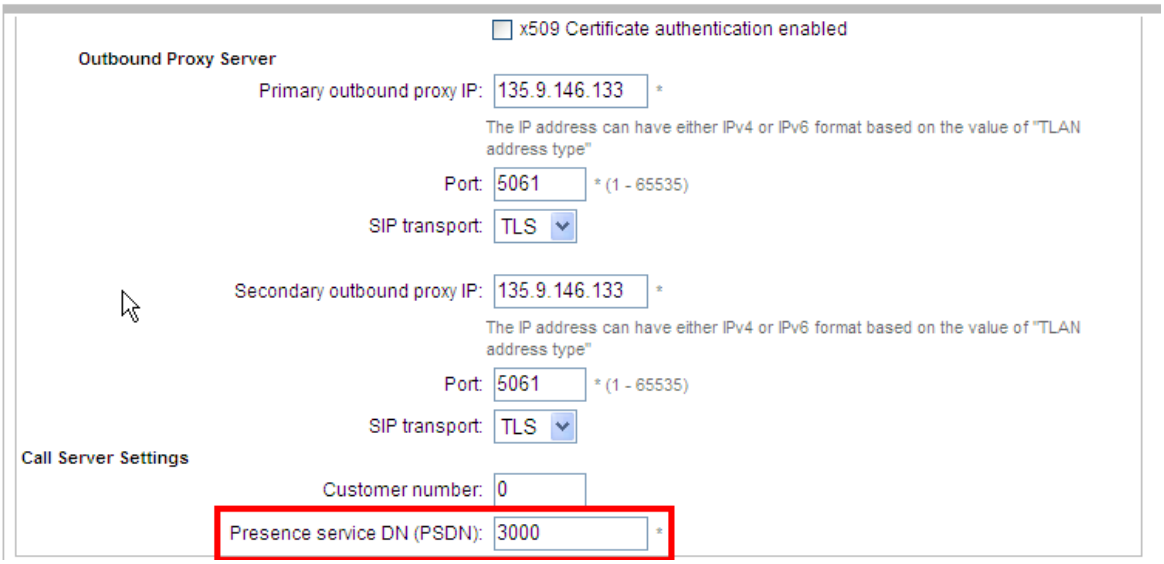
Enter in the following for the fields below shown in the screen shot. Note these are used for the reference configuration.

- Presence Publisher**: Enable**
- Type **: Aura PS**
- IM and Presence server FQDN**:** Enter the **domain** of the presence service. (not the FQDN of the Presence server. "**pres.ips.avaya.com"**
- Presence Server IP**: IP address** of the Presence Service, "**135.9.146.134**"
- Port: **15061**
- SIP Transport: **TLS** (TLS must be used for Presence)
- Presence Publisher SIP Port: **5080** (sip port must be unique to the CS1000 over the virtual trunk)
- Presence Publisher TLS Port: **5061**
- Security Policy: **Best Effort**



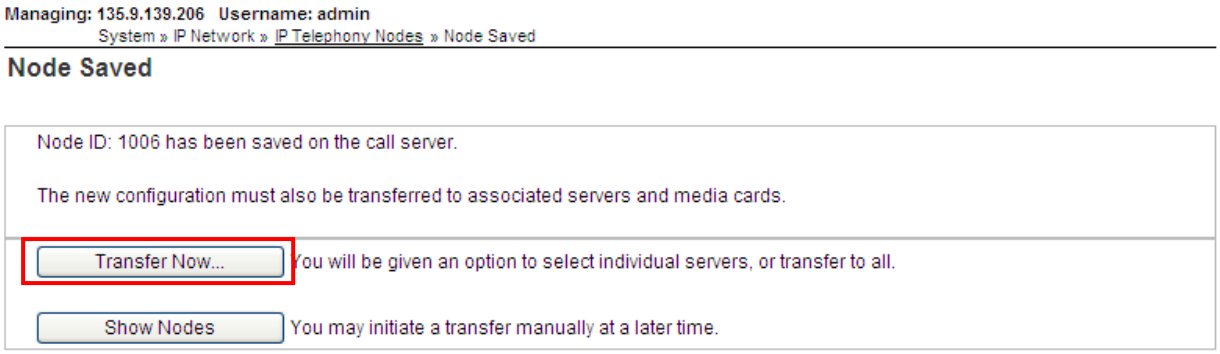
Enter in the following for the fields below shown in the screen shot. Note these are used for the reference configuration.

- Outbound Proxy: **Session Manager asset sip service IP address,** "**135.9.146.133**"
- Port: **5061**
- Transport: **TLS**
- Secondary: **5061**, **TLS** can be used as secondary transport to Session Manager
- Call Server Settings:
  Customer: **0** - Select the CS 1000 customer #
  PSDN : **Service # (DN) the CDN built** of the publisher user agent built in above section which is "**3000**".

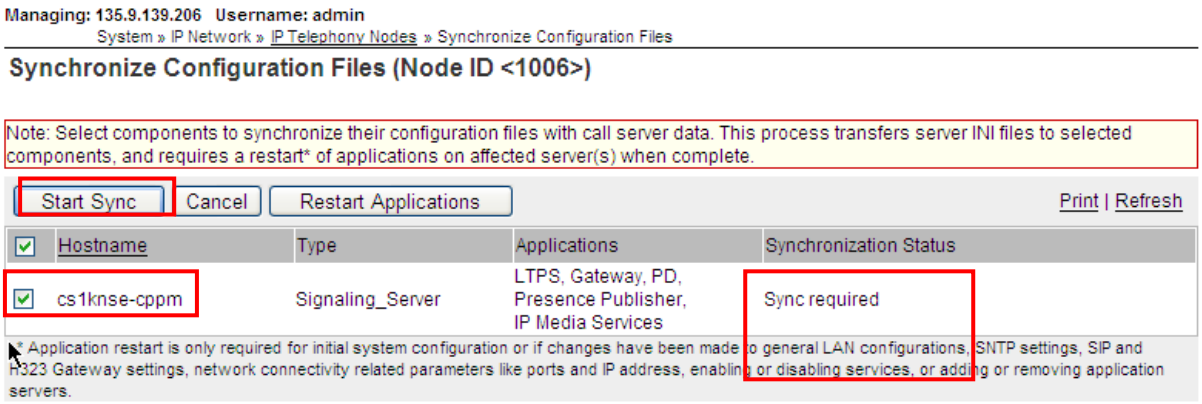


Click **Save** on the **Node Details** screen (not shown).

Select **Transfer Now** on the **Node Saved** page as shown below.



Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.



Enter ☑ associated with the appropriate Call Server and click **Start Sync.** The screen will automatically refresh until the synchronization is finished. The **Synchronization Status** field will update from **Sync required** (as shown) to **Synchronized** (not shown).

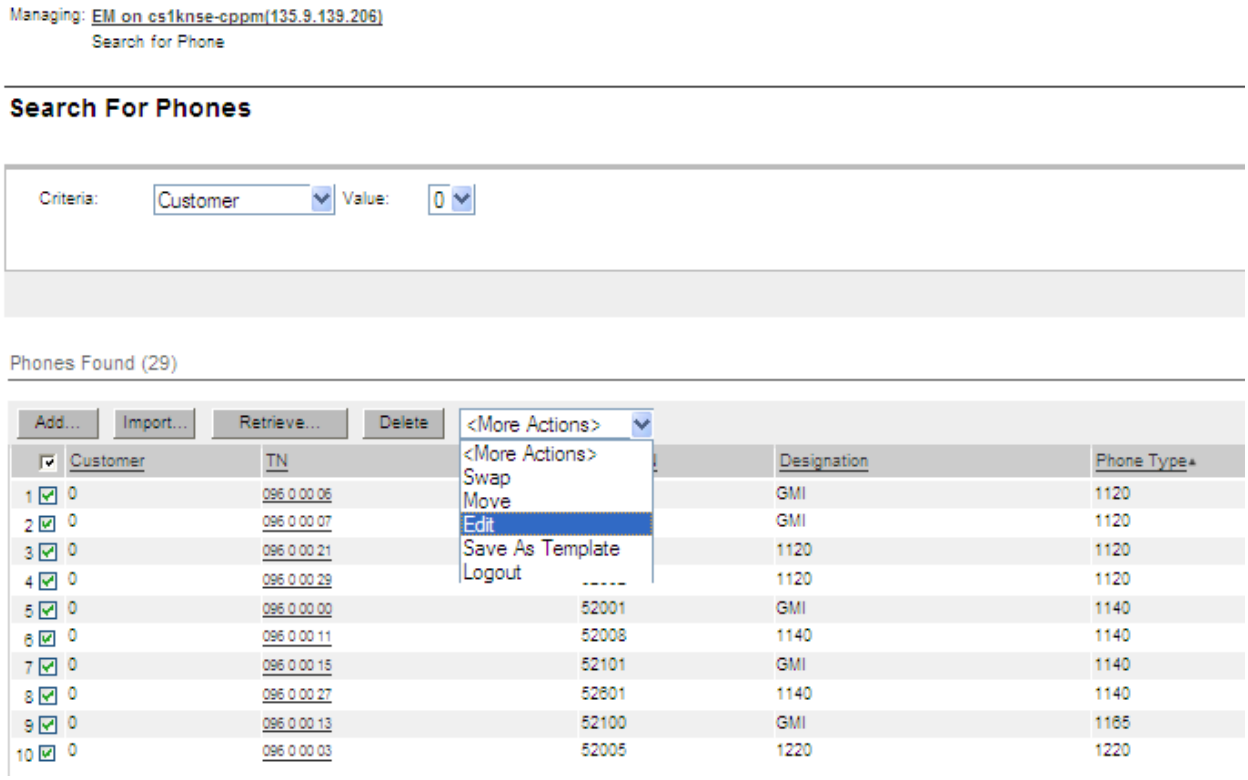
After synchronization completes, click **Restart Applications** to use new SIP Gateway settings.

4.6.6. Configure Presence Services for all Communication Server 1000 Users

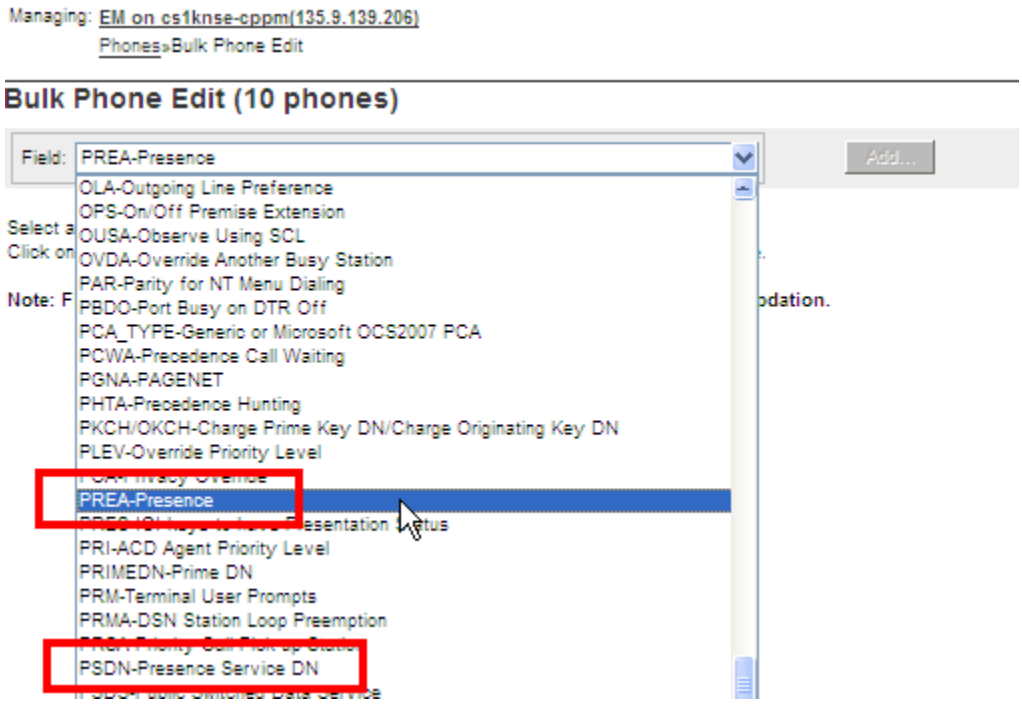
To enable Presence Services for each Communication Server 1000 user phone the following features must be configured as follows:

1. Presence Allowed (PREA) = "**Allowed**"
2. Services DN (PSDN) = "**3000**"

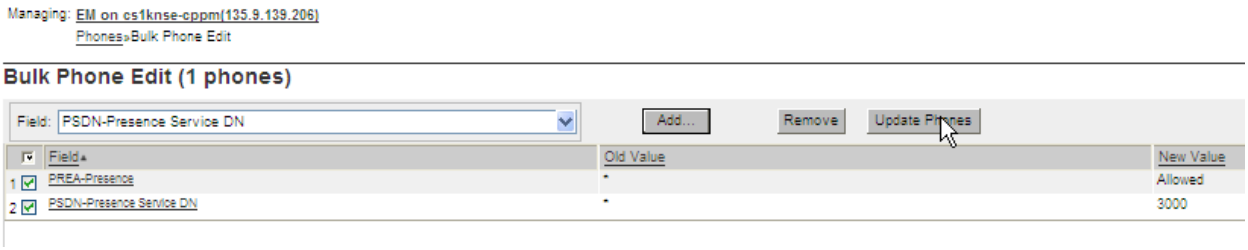
Navigate to **UCM Services - Elements – EM-Phones**. Select "Customer", Value "0" then choose all the phone types that are to be configured. Select **More Actions** "**Edit**".



Add "**PREA-Presence**" and "**PSDN-Presence Services DN**" Fields.



Select Old Value and New Value (as shown below) and select "**Update Phones**".

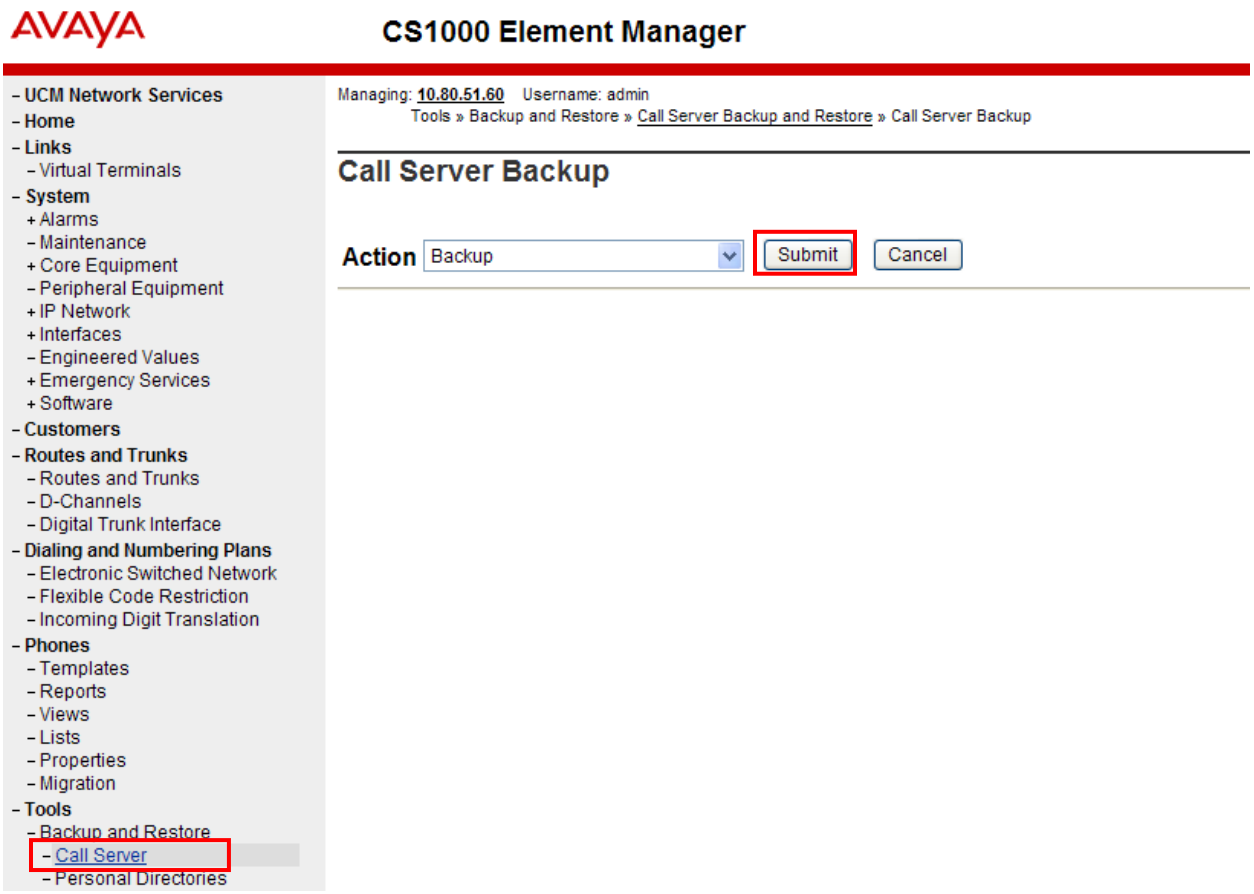


Confirm changes are successful (screen not shown).

4.7. Save Configuration

Expand **Tools → Backup and Restore** on the left navigation panel and select **Call Server.**

Select **Backup** (not shown) and click **Submit** to save configuration changes as shown below.



Backup process will take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.

Configuration of Communication Server 1000 is complete.

5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager to receive and route calls over the SIP trunk between Communication Server 1000 and the Collab Pack.

These instructions assume other administration activities have already been completed, with the Avaya Midsize Enterprise Template installation, such as defining the SIP entity for Session Manager and defining the network connection between System Manager and Session Manager. For more information on these activities, see **References [1],[2] and [3]** in **Section 12.**

Upon completion of the Avaya Midsize Enterprise Template installation and configuration the following Session Manager configuration tasks are required to align with the Communication Server 1000.

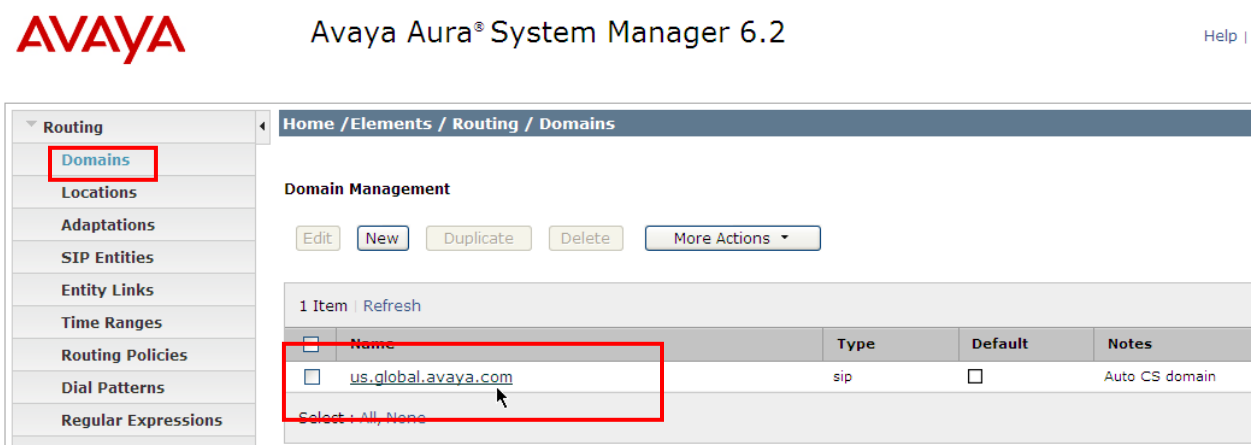
Specifically, the following administration activities will be described:

- Verify SIP Domains (with the Avaya Communication Server 1000 SIP domain)
- Define Location for Avaya Communication Server 1000
- Configure the Adaptation Module designed for Avaya Communication Server 1000 Release 7.5
- Define SIP Entities corresponding to Avaya Communication Server 1000 and Avaya Communication Manager
- Define Entity Links describing the SIP trunk and Presence link between Avaya Communication Server 1000E and Session Manager and the SIP trunk between Avaya Communication Manager and Session Manager
- Define an Entity Link describing the SIP trunk used for Presence services between the Communication Server 1000 and Session Manager.
- Define Routing Policies, which control call routing between the SIP Entities.
- Define Dial Patterns, which govern to which SIP Entity a call is routed.
- Define dial patterns for Communicator Server 1000 phones, MWI notification, PSTN access and PCA calls

Note: Some administration screens have been abbreviated for clarity.

5.1. Verify SIP Domains

Expand **Elements - Routing** and select **Domains** from the left navigation menu and verify that the Domain Name is the same as the Communication Server 1000 SIP Gateway Domain as shown in Section 4.4. In this sample configuration "**us.global.avaya.com**" was used. If the environment has pre-defined SIP domain it should be used here.



5.2. Define Location for Avaya Communication Server 1000

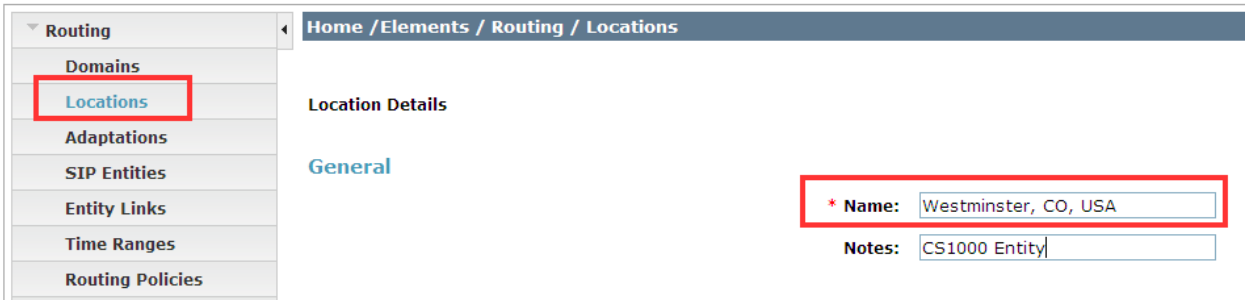
Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

Expand **Elements - Routing** and select **Locations** from the left navigational menu.

Click **New** (not shown)**.** In the **General** section**,** enter the following values and use default values for remaining fields**.**

- **Name:** Enter a descriptive name for the location.
  "**Westminster, CO, USA**" was used for reference configuration.
- **Notes:** Add a brief description. [Optional]

Click **Commit** to save.
The screen below shows the Location defined for Communication Server 1000 in the sample configuration.



5.3. Configure Adaptation Module

To enable calls between stations on Communication Server 1000 and SIP endpoints registered to Session Manager, Session Manager should be configured to use an Adaptation Module designed for Communication Server 1000 to convert SIP headers in messages sent by Communication Server 1000 to the format used by other Avaya products and endpoints. All calls to the Communication Server 1000 will have the Communication Server 1000 NARS access code ('1' is used for this reference configuration) added as they leave Communication Manager. The Session Manager will route all digit strings with a leading '1' to the Communication Server 1000. It will be necessary to delete the leading '1' for those calls that terminate within the Communication Server 1000 (station calls and Call Pilot).

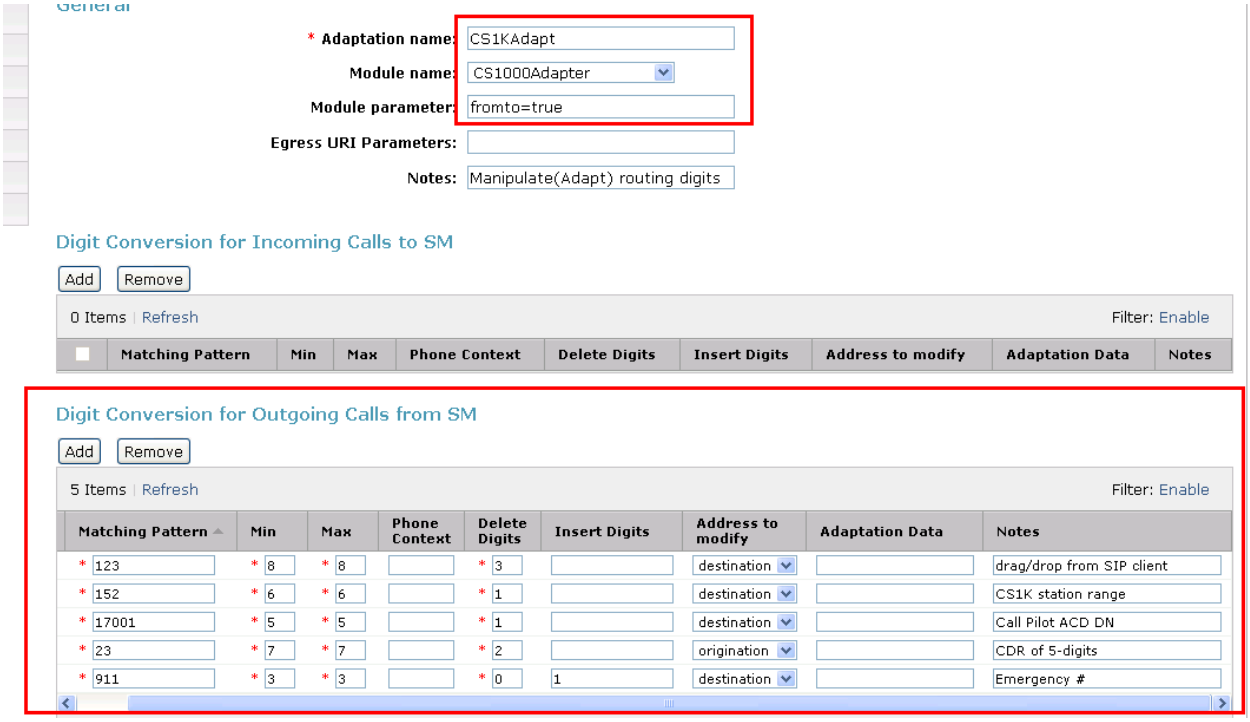
Expand **Elements - Routing** and select **Adaptations** from the left navigational menu.

Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Adaptation Name:** Enter an identifier for the Adaptation Module **Module Name:** Select "**CS1000Adapter**" from drop-down menu
- **Module Parameter: "fromto=true"** this will ensure that the 'from' header is updated In the **Digit Conversion for Outgoing from SM** section, click **Add** and enter the following values.

Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address To Modify	Notes
123	8	8	3		destination	Drag/drop from Flare Communicator Client
152	6	6	1		destination	CS 1000 Phone Range
17001	5	5	1		destination	Call Pilot DN of 7001
23	7	7	2		origination	5-digit 'from' header for CDR
911	3	3	0	1	destination	Emergency number

- Click **Commit.** The Adaptation Module defined for sample configuration is shown below.



5.4. Define SIP Entities

A SIP Entity must be added for Communication Server 1000 and Communication Manager (5.4.1)

Expand **Elements - Routing** and select **SIP Entities** from the left navigation menu.

Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

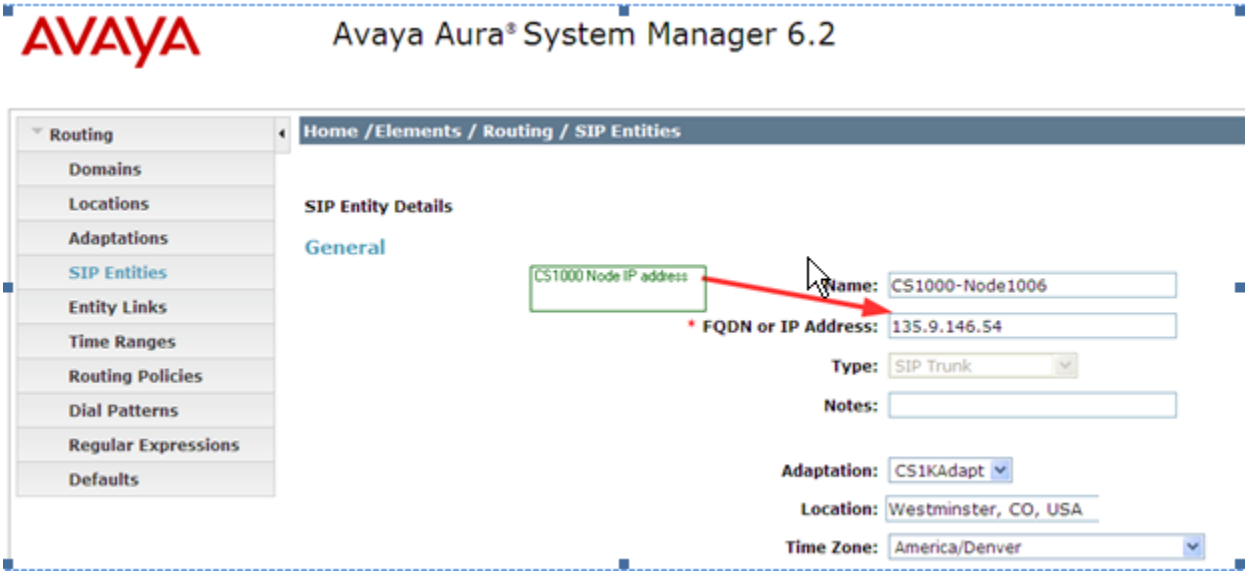
- **Name:** Enter an identifier for the SIP Entity , "**CS1000-Node 1006**"
- **FQDN or IP Address:** "Node" IP address of the CS1000 IP Telephony interface "**135.9.146.54**"
- **Type:** Select "**SIP Trunk**"
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the Adaptation Module defined above
- **Location:** Select the Location defined for Communication Server 1000 above.

In the **SIP Link Monitoring** section:

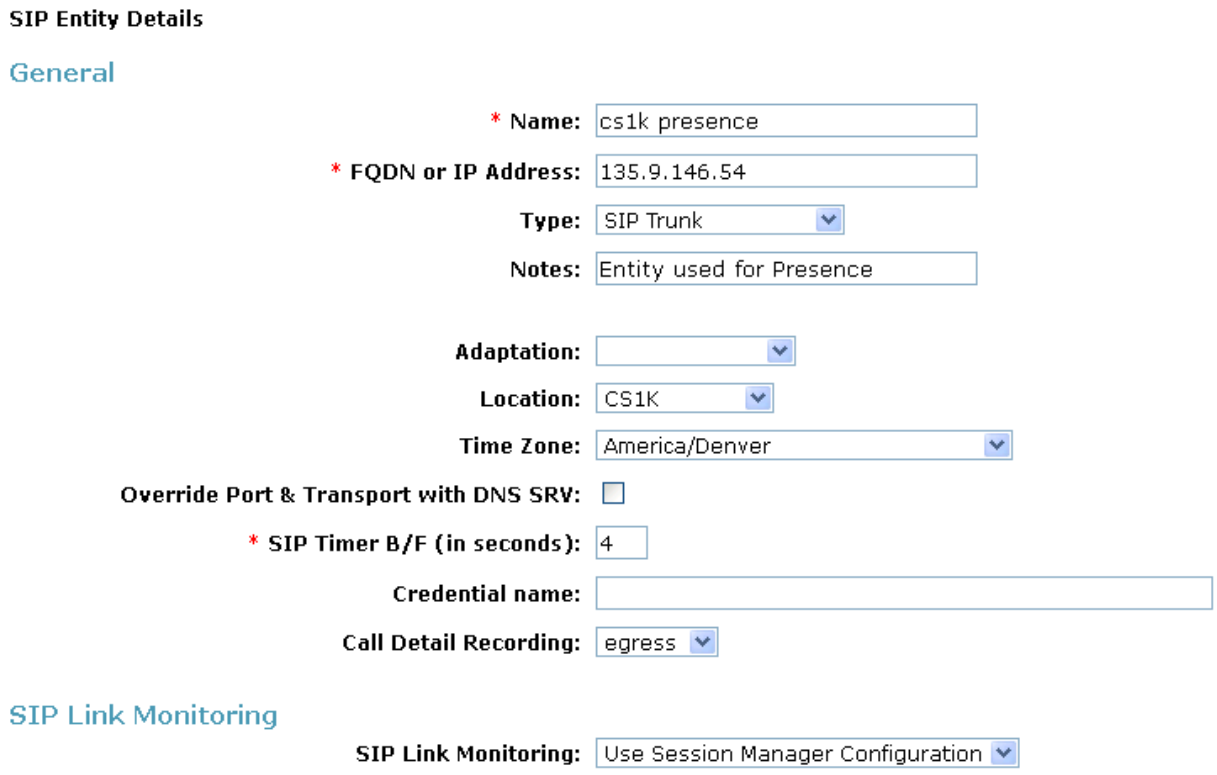
- **SIP Link Monitoring:** Select "**Use Session Manager Configuration**"

Click **Commit** to save the definition of the new SIP Entity.

The following screen shows the SIP Entity defined for Communication Server 1000 in the sample configuration.



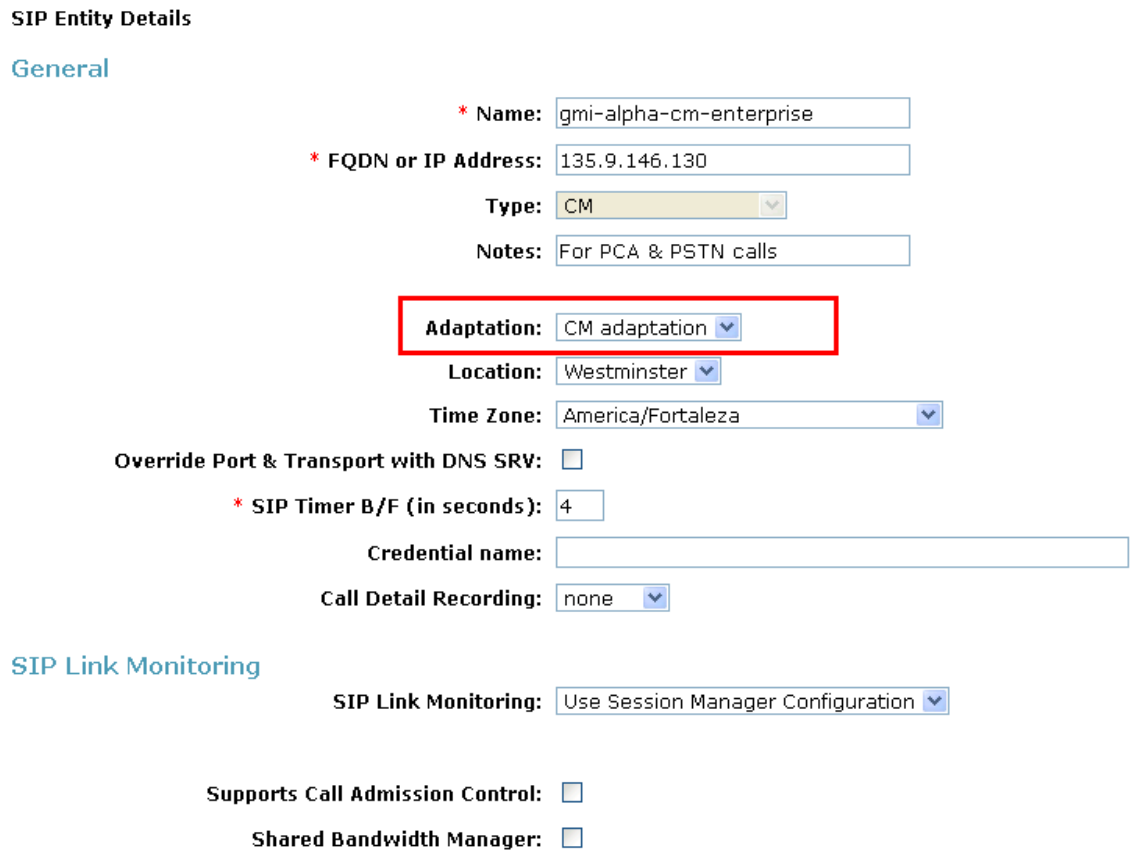
A second SIP Entity is required for the Communication Server 1000. This Entity will be associated with the TLS link required to send presence updates from the Communication Server 1000. The name will be different than the first Entity created above and no adaptation will be applied.



6.4.1 SIP Entity for Communication Manager

The SIP Entity built during the installation of the Midsize Enterprise (ME) server is required for Collaboration clients to access Communication Manager for features and is dedicated to that IMS (IP Multimedia Subsystem) functionality. A second SIP Entity is built for Communication Manager to handle Enterprise traffic (calls to/from Communication Server 1000 and calls to PSTN via Communication Server 1000). This Entity will have the same IP address as the SIP Entity built during the ME server installation. The corresponding Entity Link (5.5.1) however, will use a different TCP port and therefore a different Communication Manager SIP trunk than the SIP Entity and Entity Link built during the ME server install. This is done to ensure that Enterprise traffic can be handled separately from Collaboration client feature verification traffic and so that adaptations applied to Enterprise calling do not interfere with the IMS process. For the sample configuration, the second SIP Entity is named “gmi-alpha-cm-enterprise”.

Note: This Entity will have the Communication Manager adaptation applied whereas the Entity built during the ME server installation will not have an adaptation applied.



5.5. Define Entity Links

Any connections to Session Manager are described by an Entity Link. In the sample configuration there will be two Entity Links between Session Manager and Communication Server 1000, one for MWI/Voice traffic and one for Presence Services. Likewise, two Entity links are required between Session Manager and Communication Manager, one for Collaboration client IMS services (created during the ME server installation) and one for communication with the Communication Server 1000.

5.5.1. Entity Links Communication Server 1000

The SIP trunk between Session Manager and Communication Server 1000 is described by an Entity link.

Expand **Elements → Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

- **Name** Enter an identifier for the link to each telephony system.
- **SIP Entity 1** Select SIP Entity defined for Session Manager
- **SIP Entity 2** Select the SIP Entity defined for Communication Server

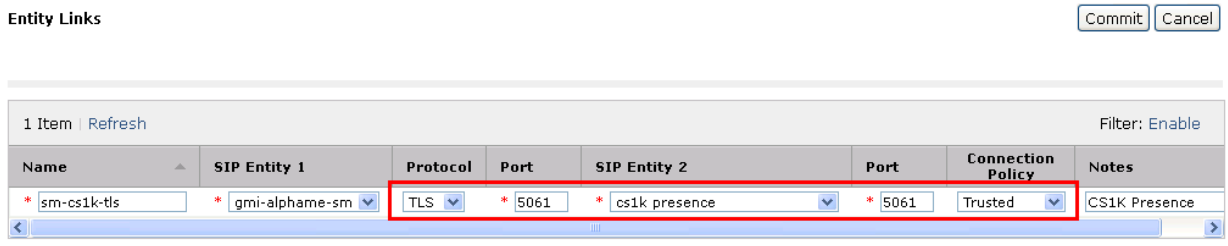
1000 for voice calls in **Section 5.4**

- **Protocol** After selecting both SIP Entities, select "**TCP"** as the required protocol.
- **Port** Verify **Port** for both SIP entities is the default listen port. The default listen port is "**5060**". Example uses TLS **5061**
- **Trusted** Enter ☑
- **Notes** Enter a brief description. [Optional]

Click **Commit** to save **Entity Link** definition.

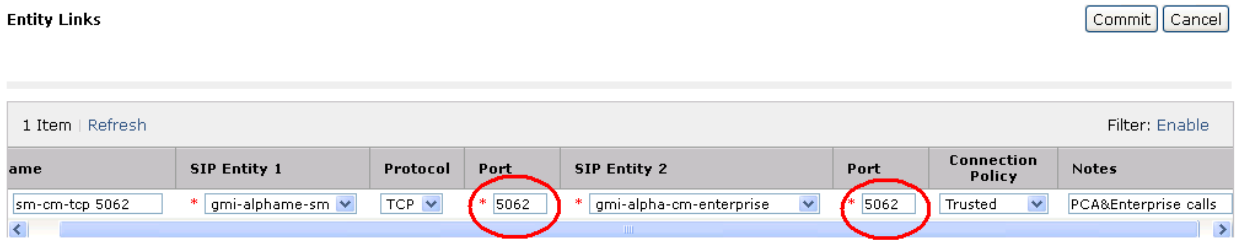
The following screen shows the entity link defined for the SIP trunk between Session Manager and Communication Server 1000 for MWI and voice traffic.

The Entity Link for Presence services will use the Entity built for Communication Server 1000 Presence in Section 5.4 and will used TLS on port 5061.



5.5.2. Entity Link for Communication Manager

The Entity Link built between Session Manager and Communication Manager during the installation of the ME server is required for the Collaboration clients to access the Communication Manager for telephony features. A second Entity Link is built between Session Manager and Communication Manager to handle Enterprise traffic (calls to/from Communication Server 1000 and calls to PSTN via Communication Server 1000). This link will use a TCP port other than that used for the Entity Link built during the ME server installation. Using a different port requires a second SIP trunk to be built in Communication Manager and ensures that any inbound or outbound digit manipulation does not affect the IMS traffic required by the Collaboration clients to function properly.



5.6. Define Routing Policy

Routing policies describe the conditions under which calls will be routed to Communication Server 1000 from either SIP endpoint registered to Session Manager. Routing Policies will also be used to send calls and Callpilot MWI notification messages from the Communication Server 1000 to the Avaya Communication Manager.

To add a routing policy, Expand **Elements - Routing** and select **Routing Policies.**

Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional]

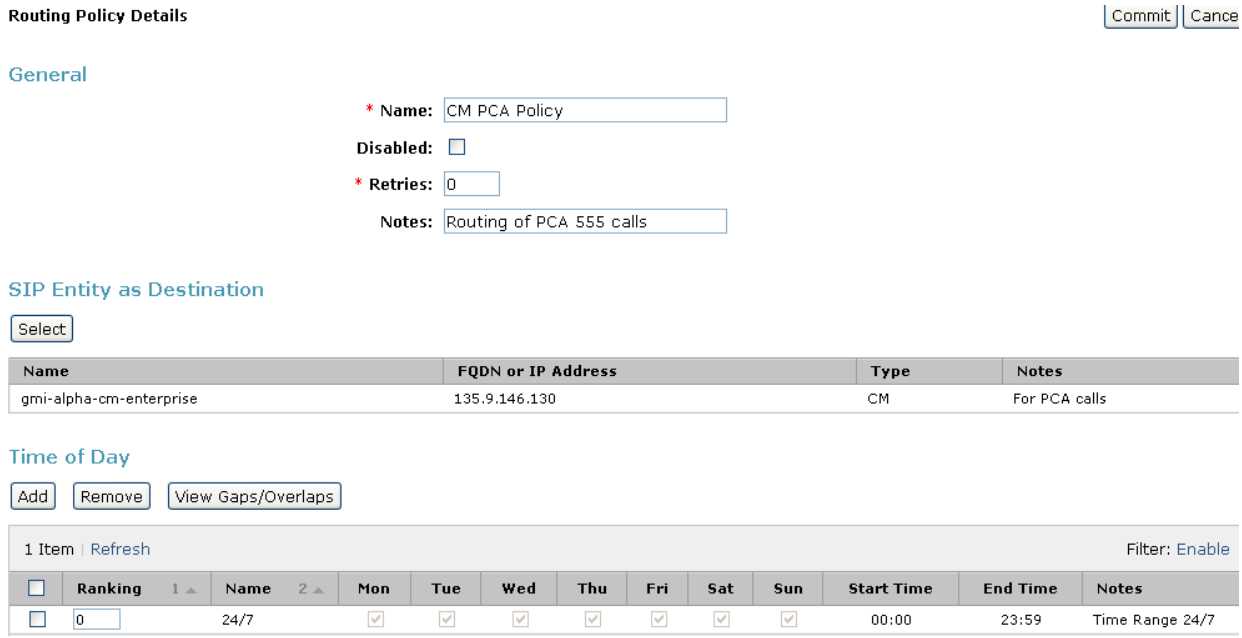
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with Communication Server 1000 as defined above and click **Select.**
- The selected SIP Entity displays on the **Routing Policy Details** page.

Use default values for remaining fields. Click **Commit** to save Routing Policy definition.
Note: The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

The following screen shows the Routing Policy for Communication Server 1000.

Following the same procedure as above, a Routing Policy is built to Communication Manager. This is shown in the following screen:



5.7. Define Dial Pattern

Dial patterns are used to route calls to appropriate SIP Entities. In the sample configuration, since stations on Communication Server 1000 were assigned extensions starting with "**52**###", calls starting with digits "52" will be routed to Communication Server 1000. Other Dial Patterns are also required for PSTN bound traffic, Communication Server 1000 traffic, MWI Notification and emergency dialing.

To define a dial pattern, expand **Elements - Routing** and select **Dial Patterns** (not shown).

Click **New,** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

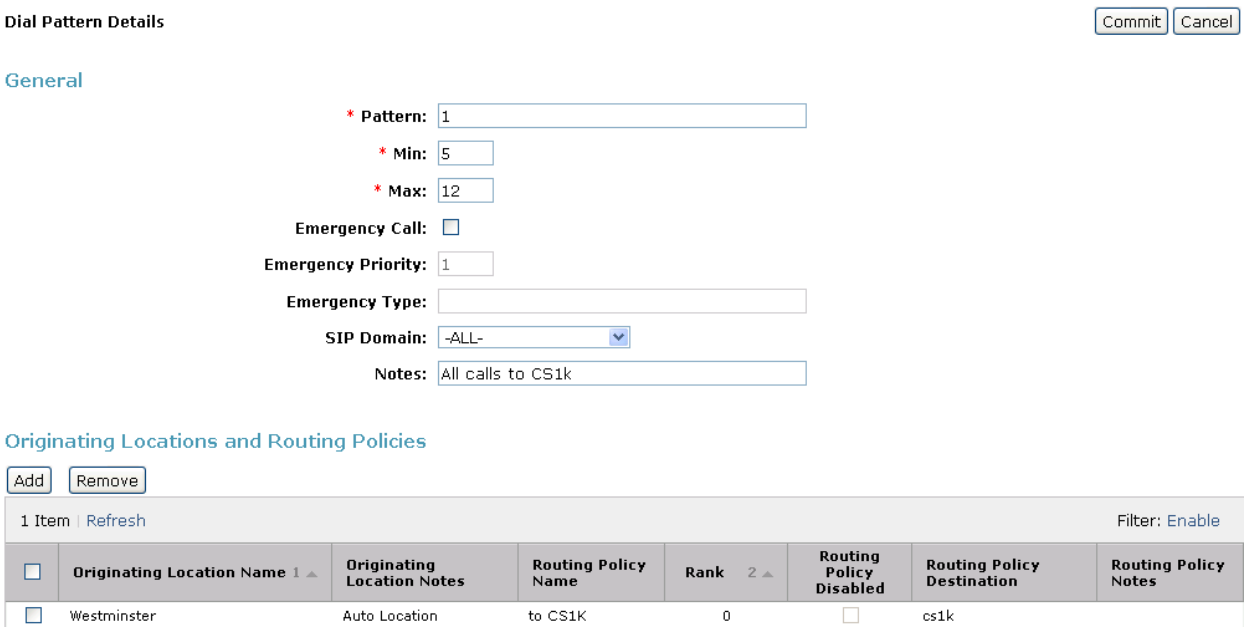
- **Pattern:** Enter dial pattern for calls to Communication Server 1000
- **Min:** Enter the minimum number digits that must to be dialed.
- **Max:** Enter the maximum number digits that may be dialed.
- **SIP Domain:** Select the SIP Domain from drop-down menu or select **"All"** if Session Manager should accept incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

In the **Originating Locations and Routing Policies** section, click **Add.**
The **Originating Locations and Routing Policy List** page opens (not shown).

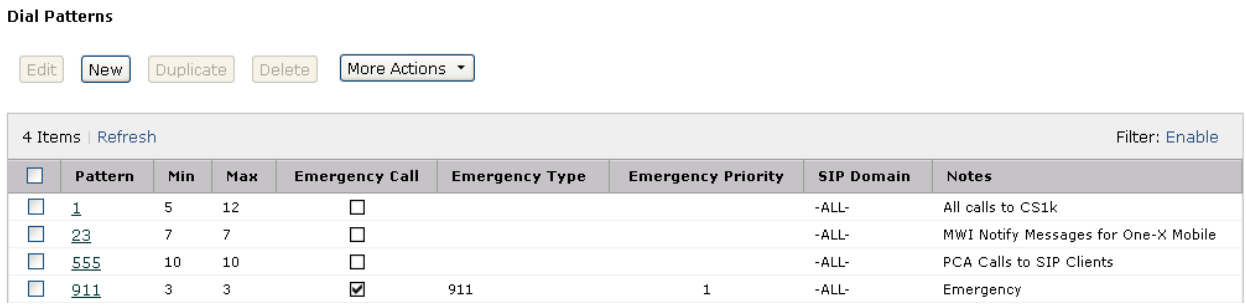
- In **Originating Locations** table, select "**ALL**"

- In **Routing Policies** table, select the Routing Policy that should be used to reoute the digits.
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save. The following screen shows the Dial Pattern defined for sample configuration. Since all calls bound for the Communication Server 1000 or PSTN via Communication Server 1000 will have a leading '1' inserted, the dial pattern for those calls is simplified into a single entry.



And the final dial pattern configuration is below:



The dial pattern '1' is used to route PSTN bound calls as well as "drag and drop spotlight calls" from Flare Communicator client, 5-digit station calls and calls to CallPilot voicemail.
The dial pattern '23' is used for MWI notifications back to the Collaboration clients. The dial pattern '555' is used for the routing of calls from Communication Server 1000 PCA calls. The routing digits used for PCA calls are arbitrary, however it is required that routing digits be used.

It is necessary to route the MWI notifications differently than the PCA calls due to the requirement for Communication Manager to handle them differently. PCA calls will be routed to ARS digit-conversion and the MWI Notify messages will not.
Summary of Dial Patterns Used in this sample configuration are:

Pattern	Min	Max	SIP Domain	Emer.	Originating Location	Routing Policy	Notes
1	8	11	-ALL-	N	Westminster	to CS1K	All non-5 digit calls to CS1k
23	7	7	-ALL-	N	CS1K	CM Policy	MWI Notify Messages for One-X Mobile
555	10	10	-ALL-	N	CS1K	CM PCA Policy	PCA Calls to SIP Clients
911	3	3	-All-	Y	Westminster	to CS1K	Emergency Calls

6. Configure Avaya Aura® Communication Manager

This section describes the concepts needed to configure Communication Manager to support Converged endpoints for Communication Server 1000 with Avaya Aura® Midsize Enterprise. These instructions assume the Avaya G430 Gateway is already configured on Communication Manager. For information on how to administer other aspects of Communication Manager, see **References [14]** and **[15]** in **Section 12.**

The following administration steps will be described:

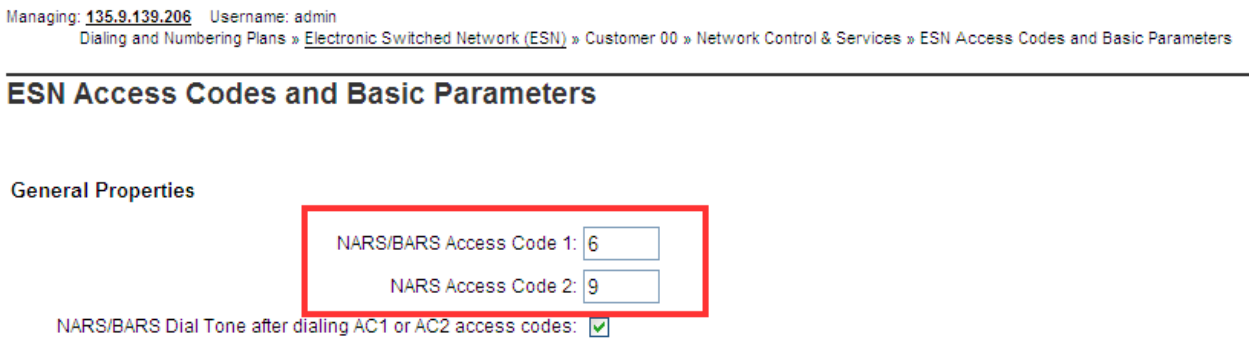
- Verify System Access codes match
- Verify - IP Network Region – SIP Domain
- Enable Trunk to Trunk transfers
- Administer Private, Public Numbering Plan and Uniform Dial plan
- Administer AAR/ARS Analysis
- Administer Dial Plan Analysis
- Administer Dial Plan Parameters
- Administer a Route Pattern
- Administer a SIP Trunk/Signal Group
- Administer Incoming Call Handling

6.1. Verify System Access Codes match

To allow users to utilize Converged dialing plans to route calls, verify the Communication Manager AAR and ARS access codes match Communication Server 1000 Access Codes.

Verify Communication Server 1000 Access Codes:

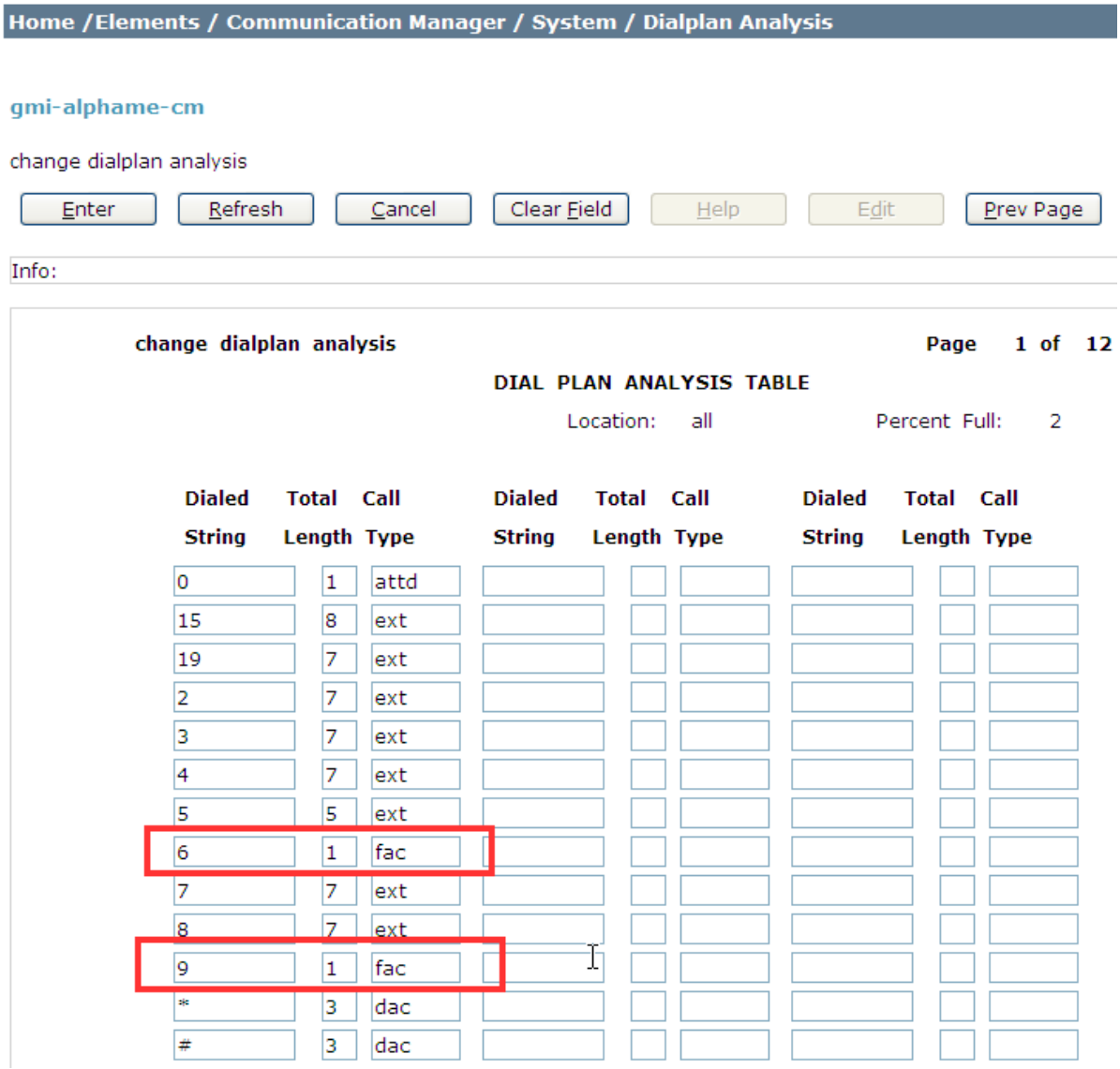
Navigate to **UCM Services – EM – ESN** – **ESN Access Codes and Parameters**



In the **Dialplan Analysis** change your dialed string to match Feature Access Code (FAC) examples "**9**" and "**6**".

Using SMGR-Elements-Communication Manager-System-Dialplan Analysis

- Dialed String 6
- Total Length 1
- Call Type FAC—identifies this 1-digit number as a Feature Access Code
- Repeat steps to add digit ‘9’ as FAC



Using SMGR-Elements-Communication Manager-System-Feature Access Codes
On page 2 of Feature Access Codes, verify ‘9’ is defined as ARSFAC1

Feature Access Codes List

View | Edit | New

36 Items | Refresh | Show 15 | Filter: Enable

	Feature Access Code	Description	System
○	#51	Enhanced EC500 Deactivation	gmi-alphame-cm
○	*51	Enhanced EC500 Activation	gmi-alphame-cm
○	*50	EC500 Self-Administration AC	gmi-alphame-cm
○	*61	Directed Call Pickup AC	gmi-alphame-cm
○	#80	Contact Closure Close Code	gmi-alphame-cm
○	*80	Contact Closure Open Code	gmi-alphame-cm
○	*42	CAS Remote Hold/Answer Hold-Unhold AC	gmi-alphame-cm
○	*41	CCall Pickup Access Code	gmi-alphame-cm
○	*40	Call Park Access Code	gmi-alphame-cm
○	#30	Call Forwarding Deactivation	gmi-alphame-cm
○	*31	Call Forwarding Activation	gmi-alphame-cm
○	*30	Call Forwarding Activation Busy/DA	gmi-alphame-cm
○	#33	Automatic CallBack Deactivation	gmi-alphame-cm
○	*33	Automatic CallBack Activation	gmi-alphame-cm
○	9	ARSFAC1	gmi-alphame-cm

On page 3 of Feature Access Codes, select AARFAC and choose ‘Edit’
Add ‘**6’** in Auto Alternate Routing Field

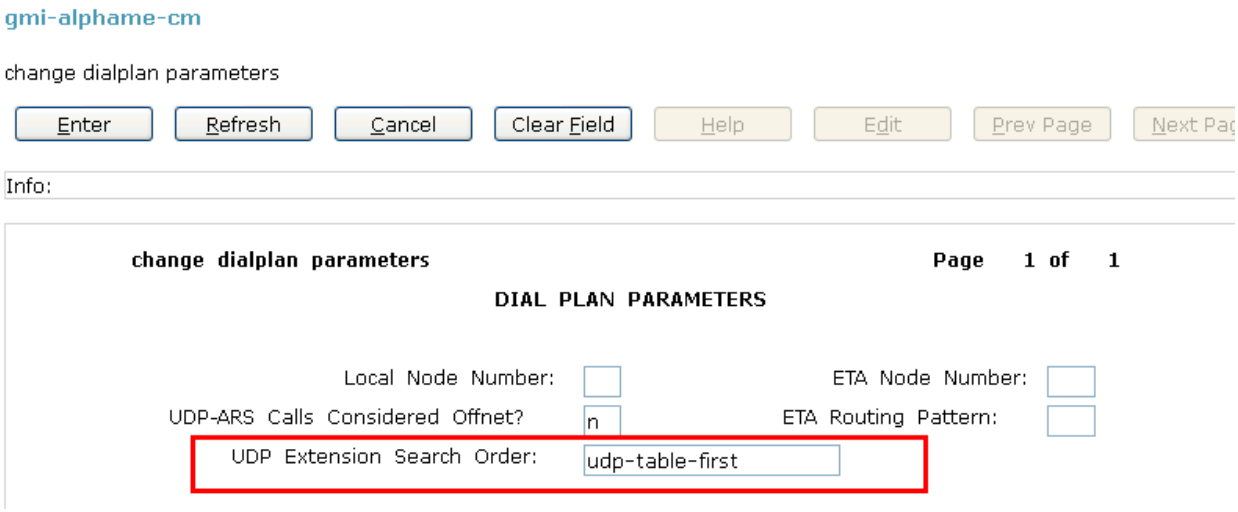
```
change feature-access-codes                                  Page   1 of  10
                          FEATURE ACCESS CODE (FAC)
          Abbreviated Dialing List1    Access Code:  *10
          Abbreviated Dialing List2    Access Code:  *12
          Abbreviated Dialing List3    Access Code:  *13
Abbreviated Dial - Prgm Group List     Access Code:  *14
                      Announcement     Access Code:  *19
                      Answer Back      Access Code:

          Auto Alternate Routing (AAR) Access Code:  6
```

Navigating to System Manager-Elements-Communication Manager-System-Dialplan Parameters

Select the item and choose ‘Edit’:

UDP Extension Search Order udp-table-first



6.2. Verify IP Network Region - Domain

Navigate to **Elements** – **Communication Manager** – **Network** and Select the **Network Region**. Enter the following values and use default values for remaining fields.

- **Authoritative Domain:** Enter the correct SIP domain for the configuration. For the reference configuration, "**us.global.avaya.com**" was used.
- **Name:** Enter descriptive name.

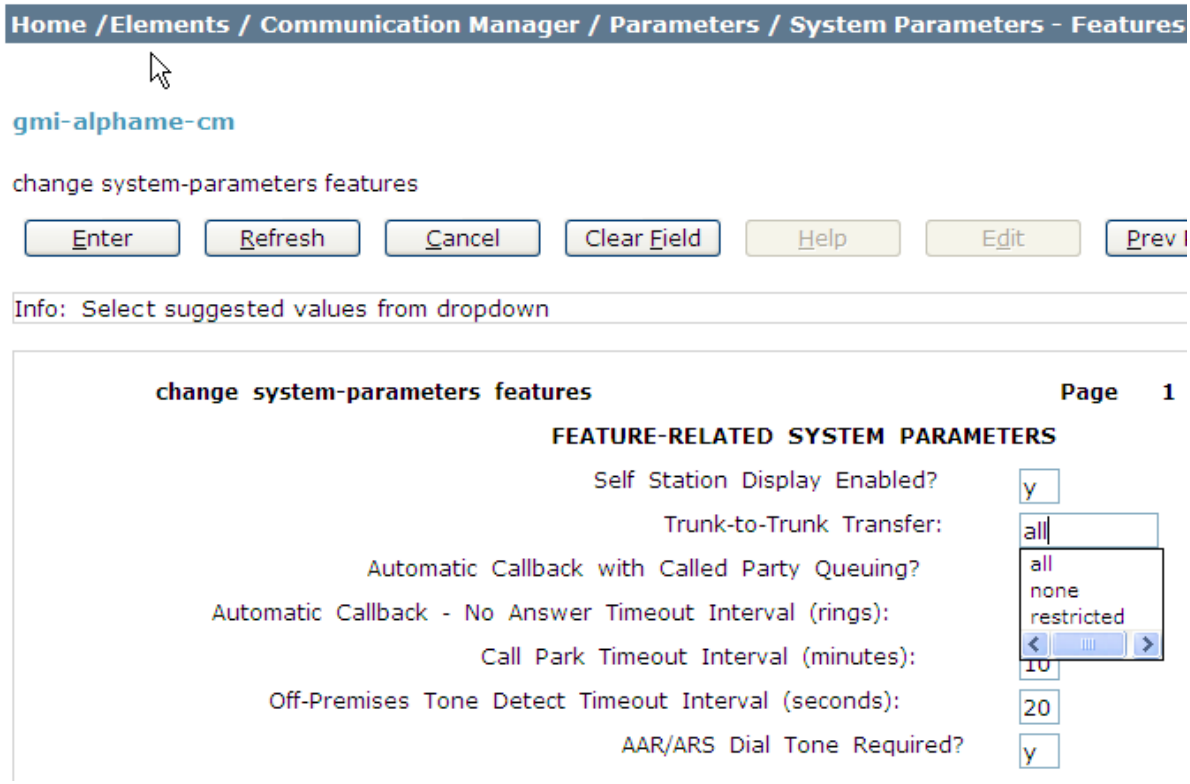
6.3. Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable trunk-to-trunk transfers. This feature is needed when an incoming call to a SIP station is transferred to another SIP station. For simplicity, the **Trunk-to-Trunk Transfer** field on **Page 1** was set to "**all**" to enable all trunk-to-trunk transfers on a system wide basis.

Note: Enabling this feature poses significant security risk by increasing the risk of toll fraud, and must be used with caution. To minimize the risk, a COS could be defined to allow trunk-to-trunk transfers for specific trunk group(s). For more information regarding how to configure Communication Manager to minimize toll fraud, see **Reference [16]** in **Section 12.**

Navigate to **Elements – Communication Manager – Parameters-System Parameters – Features**.
Select "**True".**

Select edit,
choose“all”.



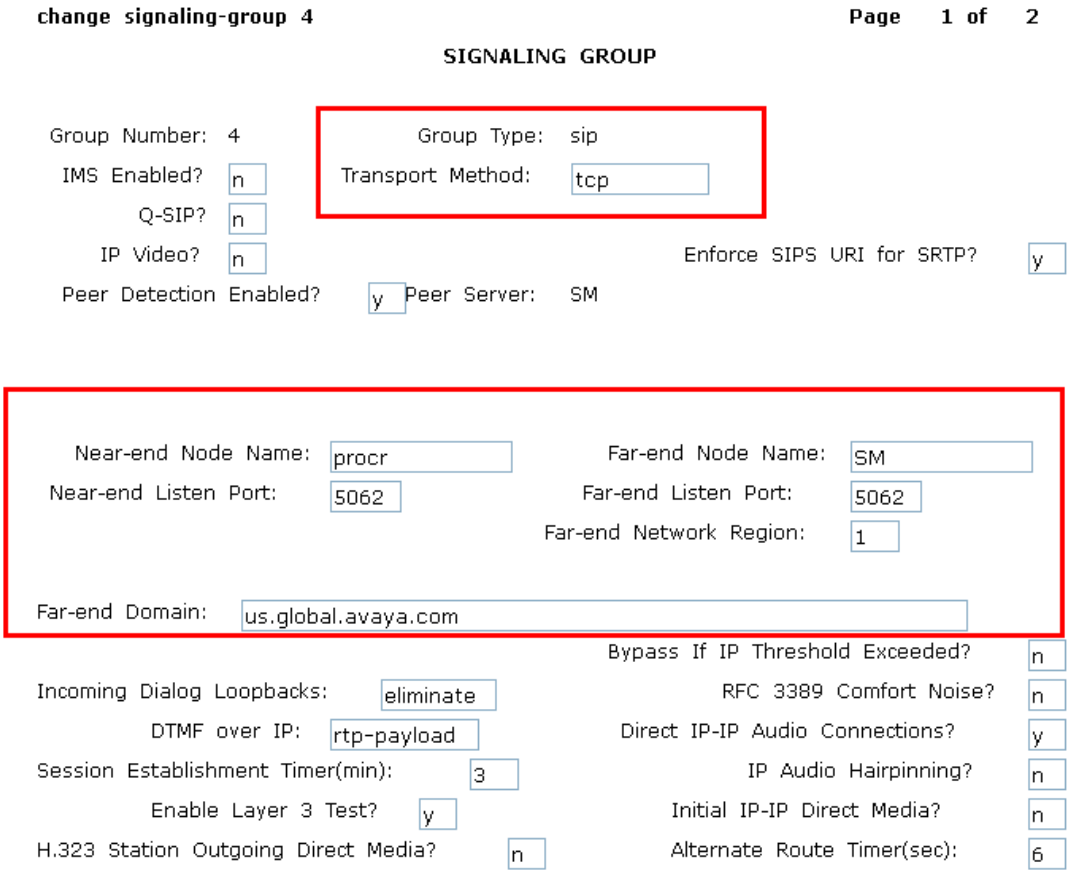
6.4. Administer Signal Group

Signal Group 4 and the associated SIP Trunk Group 4 will be used for all traffic to the Communication Server 100.

Navigate to System Manager-Elements-Communication Manager-Network-Signaling Groups-Select New

- Qualifier “4” This is the signal group number, select Add
- Group Type SIP
- Transport Method TCP—alternatively, TLS can be used
- Near-End Node Name procr—this name is created during the ME server install
- Far-End Node Name SM—this name is created during the ME server install
- Near-End Listen Port 5062—needs to be a different port than signal group 3
- Far-End Listen Port 5062—needs to be a different port than signal group 3
- Far-End Network Region 1
- Domain us.global.avaya.com—replace with SIP domain

Signal Group form should appear as below:



Select Enter.

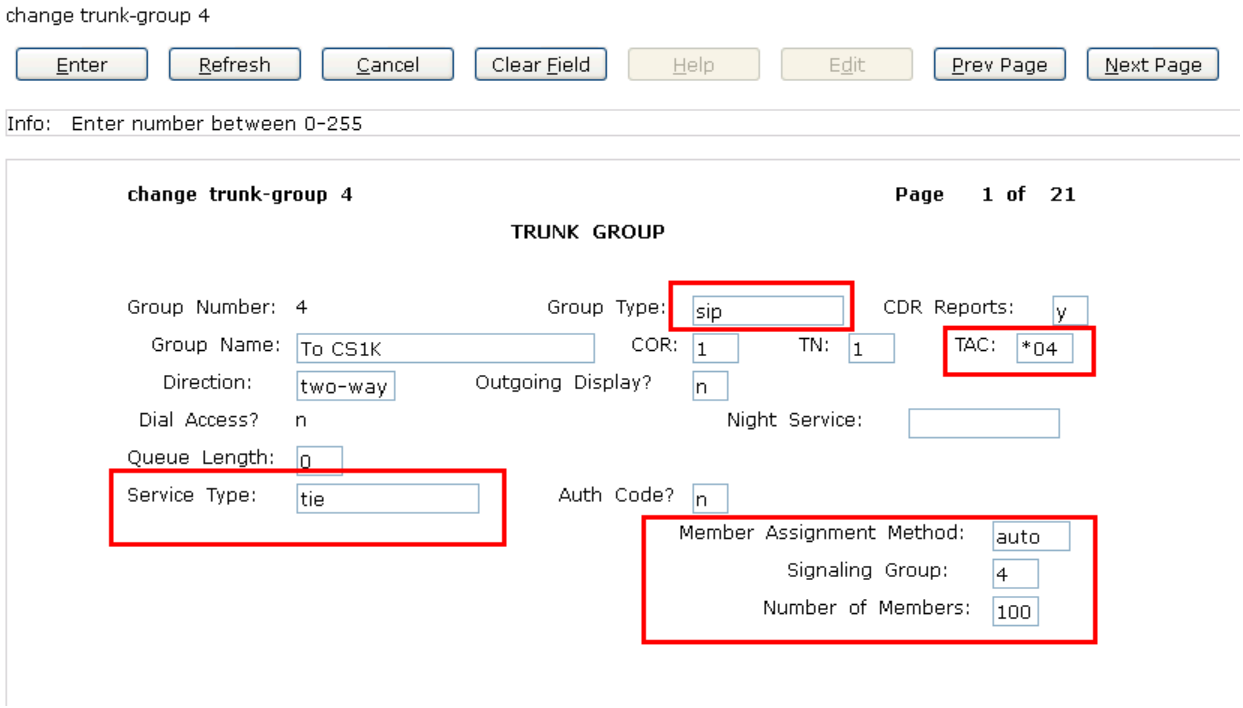
6.5. Administer SIP Trunk Group

Trunk Group 4 will use signal group 4 created in section 6.4 and will be used for all traffic to the Communication Server 1000.

Navigate to System Manager-Elements-Communication Manager-Network-Trunk Group- Select New

- Qualifier “4” This is the trunk group number, select Add
- Group Type SIP
- Group Name free text up to 27 characters (‘To CS1K’ in this config)
- TAC *04—this is the trunk access code
- Service Type TIE
- Assignment Method auto
- Signal Group 4—signal group number created in section 7.4
- Number of Members 50

Trunk Group form should appear as below:



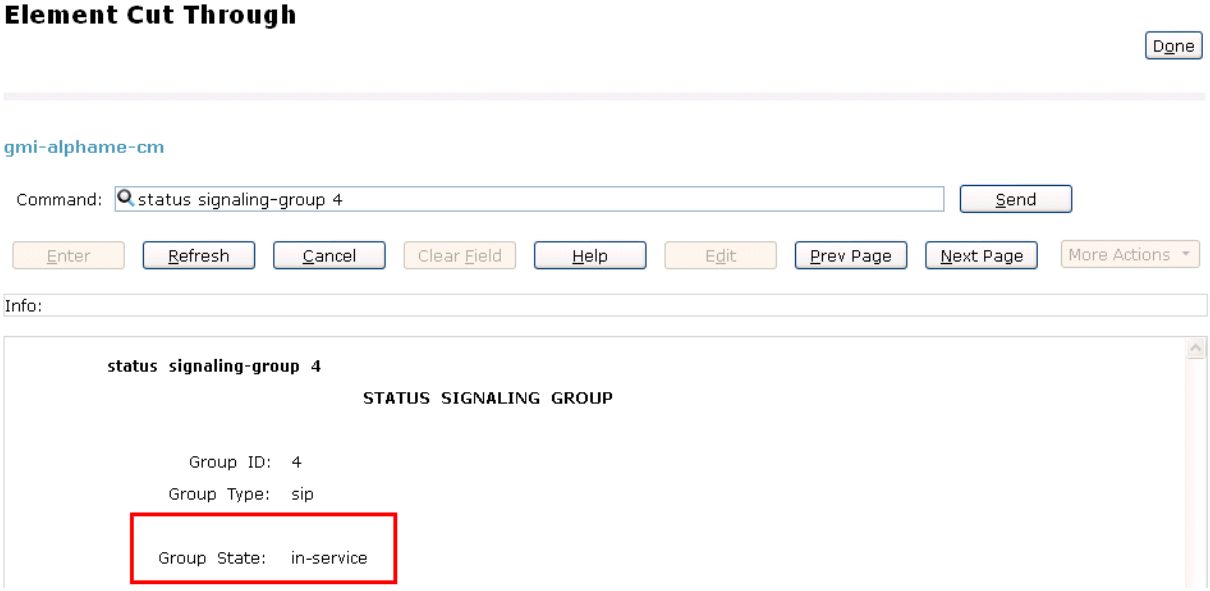
Select Enter.

6.6. Verify Signal Group and Trunk Group are In-Service

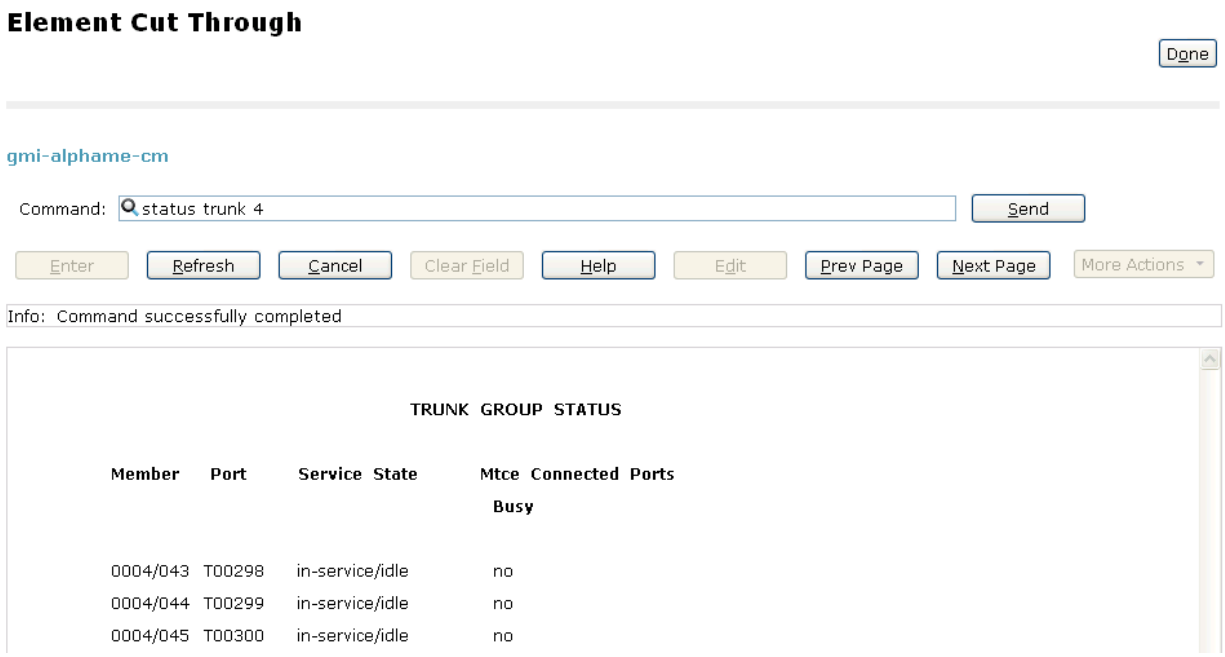
After Signal Group 4 and Trunk Group 4 have been added, ensure that both are up and in-service.

Navigating to System Manager-Elements-Inventory-Synchronization-Communication System--Launch Element Cut Through

Type ‘status signaling-group 4’
Results should be as below “in-service”



Type ‘status trunk 4’
Results should be as below ‘in-service/idle’ and ‘Mtce Busy = no’ for all 100 members (use Next Page to verify)



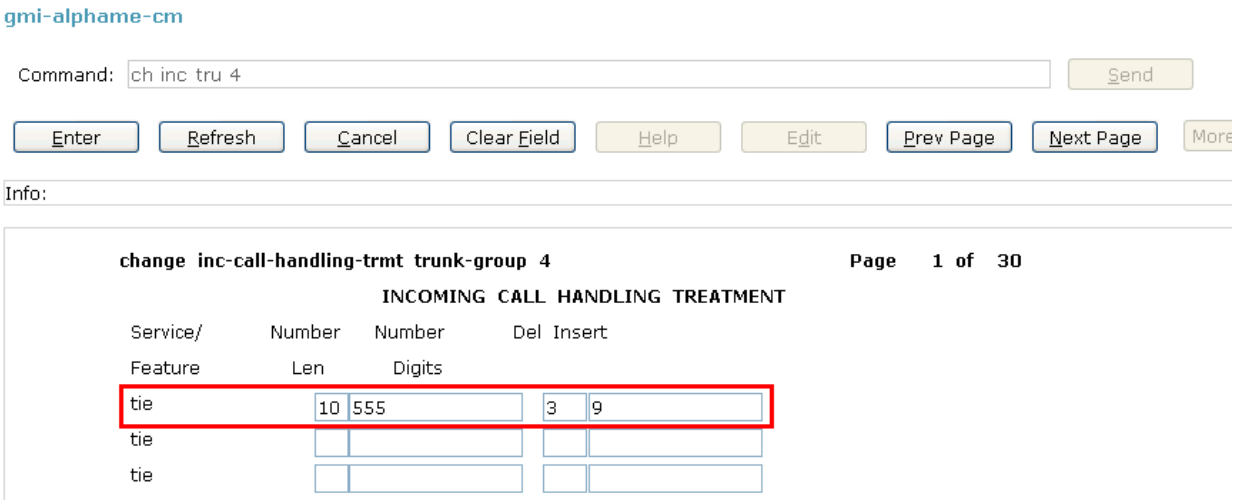
6.7. Configure Incoming Call Handling for Trunk Group

In order to strip the routing digits of '555' for PCA calls from the Communication Server 1000 to Collaboration clients, an Incoming Call Handling Rule is needed on the trunk group in Communication Manager. The Insert of '9' will route the call to ARS where ARS digit-conversion will keep it local rather than looping back to the Communication Server 1000.

Navigating to System Manager-Elements-Inventory-Synchronization-Communication System--Launch Element Cut Through

Type "change incoming tru 4"

- **Number Len 10**
- **Number Digits 555**
- **Del 3**
- **Insert 9**



6.8. Verify IP Network Region - Domain

Use the **change ip-network-region n** command where **n** is an available network region.

Enter the following values and use default values for remaining fields.

- **Authoritative Domain:** Enter the correct SIP domain for the configuration.

  For the sample configuration, "**us.global.avaya.com**" was used.
- **Name:** Enter descriptive name.
- **Codec Set:** Enter the number of the IP codec set **1** above
- **Intra-region IP-IP Direct Audio:** Enter "**yes**".
- **Inter-region IP-IP Direct Audio:** Enter "**yes**".

6.9. Administer Private Numbering Plan (

The full extension numbers used for the collaboration clients registered to Session Manager must be added to the private numbering table on Communication Manager. For the reference configuration, private numbering was used and all extension numbers were unique within the private network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in **Reference [14]** in **Section 12**.
Use the **change private-numbering n** command, where **n** is the length of the private number. Fill in the indicated fields as shown below.

- **Ext Len**: Enter length of extension numbers.
  In the sample configuration, "**7**" was used.
- **Ext Code**: Enter leading digit (s) from extension number.
  In the sample configuration, "**235xxxx**" were used for SIP endpoints.
- **Trk Grp(s):** Enter trunk groups or leave blank to use format on all trunk groups
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is

defined in Session Manager. If so, enter the appropriate prefix.

- **Total Length:** Enter "**7**" since a private prefix was not defined.

```
change private-numbering 7                                    Page   1 of  2
                            NUMBERING - PRIVATE FORMAT

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 7  23             3                           7    Total Administered: 3
```

6.10. Administer Public Numbering Plan

The full extension numbers used for the collaboration clients registered to Session Manager must be added to the public numbering table on Communication Manager. For the sample configuration, public numbering was used and all extension numbers were unique within the public network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in **Reference [14]** in **Section 12**.
Use the **change public-numbering n** command, where **n** is the length of the number.
Fill in the indicated fields as shown below.

- **Ext Len**: Enter length of extension numbers.
  In the sample configuration, "**7**" was used.
- **Ext Code**: Enter leading digit (s) from extension number.
  In the sample configuration, "**235xxxx**" were used for SIP endpoints.
- **Trk Grp(s):** Enter trunk groups or leave blank to apply for all trunks.
- **Public Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix.
- **Total Length:** Enter "**5**" since a private prefix was not defined.

These settings will ensure that a 7-digit station will show a 5-digit Calling Party Number (CPN) on outbound calls. For example, SIP extension "2352001" will show a Calling Party Number of "**52001**".

```
change public-unknown-numbering 7                             Page   1 of  2
                            NUMBERING - PUBLIC FORMAT

Ext Ext            Trk        Public Ukn          Total
Len Code           Grp(s)     Prefix           Len
 7  2              4          1303             5    Total Administered: 1
```

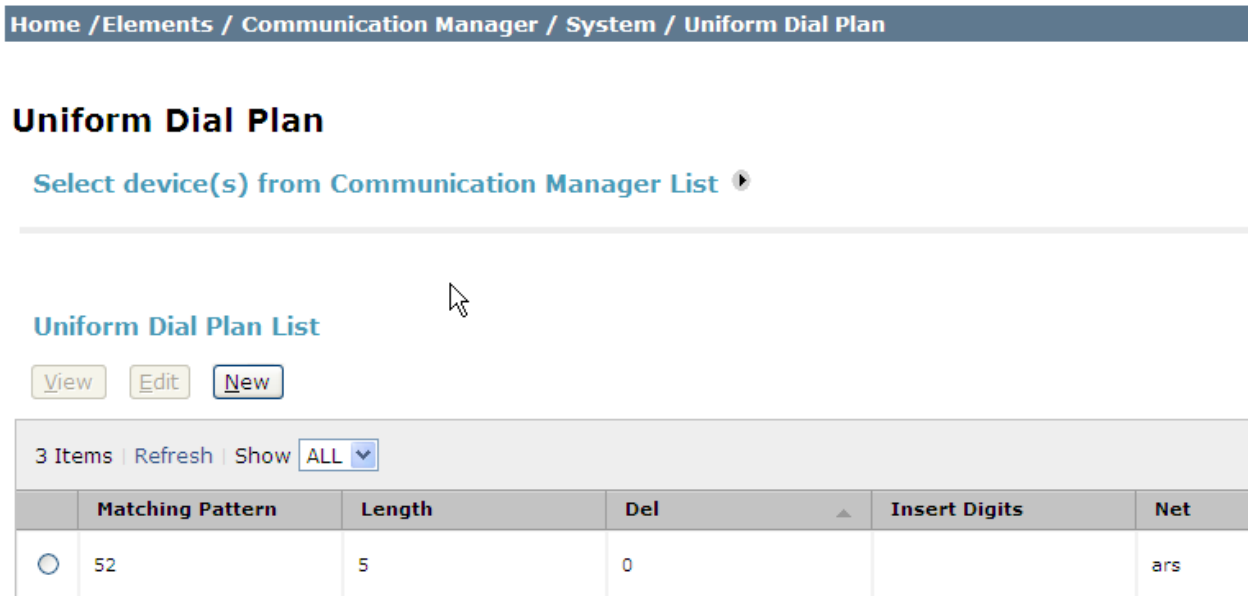
6.11. Administer Uniform Dial Plan

Navigate to **Elements** – **Communication Manager** – **System** – **Uniform Dial Plan** and add dialing plan extension range (s). In the reference configuration, 7-digit extension numbers starting with "**235xxxx**" was used for the collaboration clients associated and **52xxx** is used as the uniform dialing plan for Converged Users dialing across Communication Server and the Collab Pack.

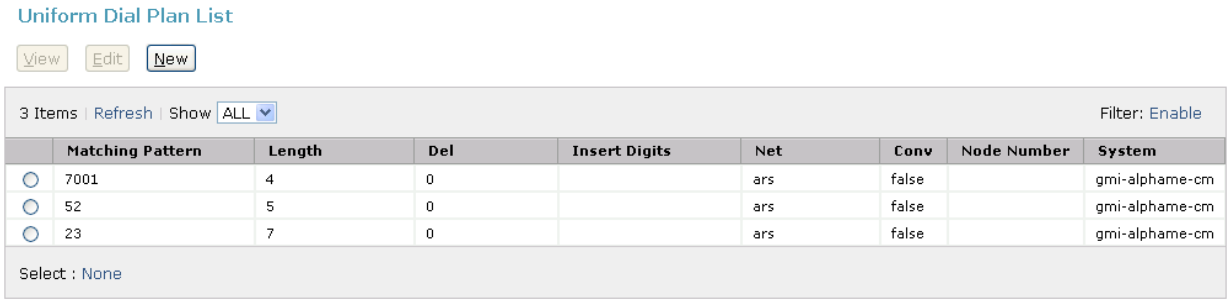
Fill in the indicated fields as shown below and use default values for remaining fields.

- **Matching Pattern** Enter digit pattern of extensions assigned to SIP endpoints (Collaboration clients) and Communication Server 1000 endpoints.
- **Len** Enter extension length.
- **Net** Enter "**ars**".

Navigate to **Elements – CM –System – Uniform Dial Plan.**



The above example is for the Communication Server 1000 station range. Following the same procedure as above, add an entry that represents the pattern range for the SIP clients (**23xxx** in this sampe configuration) and the CallPilot access number (**7001**) as in this sample configuration..
The completed Uniform Dial Plan Table is represented in the following screen:

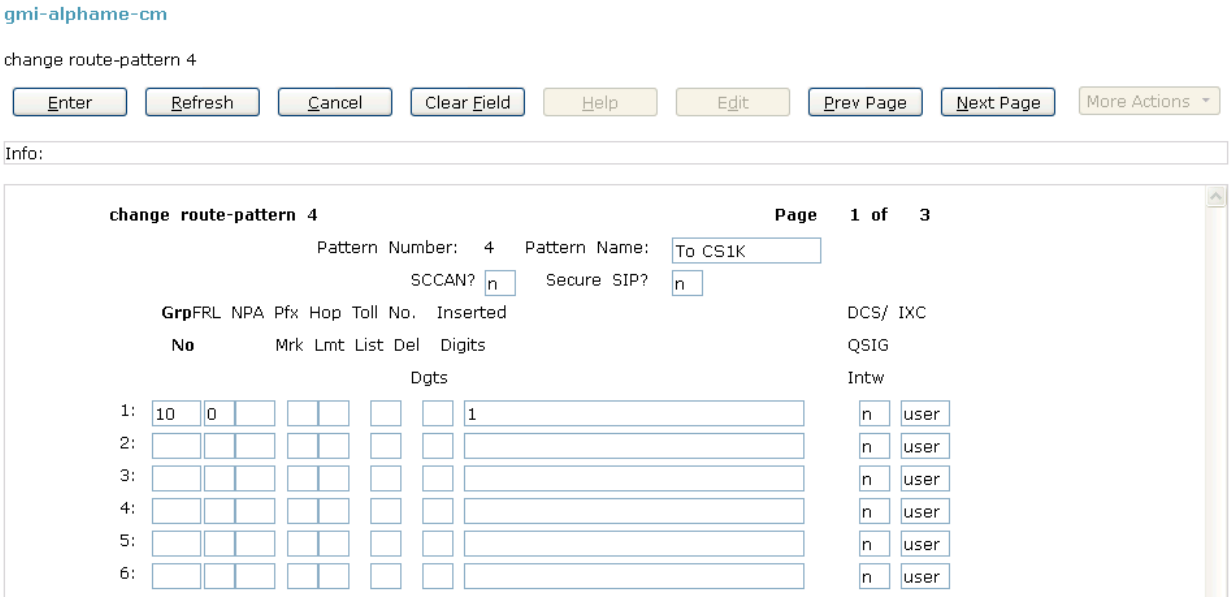


6.12. Administer Route Pattern

This section provides the configuration of the Route Pattern used in Communication Manager for the routing of calls to the Communication Server 1000, Call Pilot and PSTN via Communication Server 1000. All calls from ARS will use this route pattern 4. Route Pattern 3 is created during the ME server installation and is dedicated for the IMS signaling required by the Collaboration clients. Using a separate route pattern (route pattern 4 in this sample configuration) allows for digit manipulation on enterprise calls without affecting the IMS traffic that is using Route Pattern 3.

Navigating to System Manager-Elements-Communication Manager-Network-Route Pattern-Select New

- Qualifier "4" This will be the route pattern number
- Name Free-text up to 15 characters (To CS1K in this sample configuration)
- Grp No "4" This is the trunk group number to be used for this route
- Inserted Digits "1" Lead routing digit that SM will use to point the call to CS1K
- FRL "0" The minimal facility access code restriction



6.13. Administer ARS Analysis

This section provides the configuration of the ARS pattern used in the reference configuration for routing calls between collaboration clients and Communication Server 1000 stations, Call Pilot and to the PSTN via Communication Server 1000. All traffic that is bound for the PSTN must have dialed strings defined here as well as any digit strings pointed to ARS via the UDP table in section 6.7 (23x-xxxx, 52xxx and 7001 for this sample configuration). The ARS table needs to mimic the dialing rules of the Communication Server 1000 including local, long distance, toll-free and emergency dialing. All dialed numbers identified on the ARS table will be sent to Session Manager and routed to the Communication Server 1000 via Route pattern 4 created in section 6.8.

e.g. **52001** is the 5-digit number of a Communication Server 1000 station

- **Dialed String** Enter leading digit (s) of extension numbers, "**5**"
- **Min** Enter minimum number of digits that must be dialed. "**5**".
- **Max** Enter maximum number of digits that may be dialed. "**5**"
- **Route Pattern** Enter Route Pattern of "**4**"
- **Call Type** Enter "**locl**".

The completed ARS table below describes a dialing plan that supports local 7-digit dialing, 1+10 long distance dialing and 1+10 toll-free dialing. Since the drag/drop calling feature from the contact fan of the Flare Communicator client will be dialing 7-digits to other SIP client users that is accounted for in the ARS table as well.

Automatic Route Selection Analysis List

View | Edit | New

11 Items | Refresh | Show ALL | Filter: Enable

Dialed String	Total Min	Total Max	Route Pattern	Location	System
1	11	11	4	all	gmi-alphame-cm
2	7	7	4	all	gmi-alphame-cm
3	7	7	4	all	gmi-alphame-cm
4	7	7	4	all	gmi-alphame-cm
5	7	7	4	all	gmi-alphame-cm
5	5	5	4	all	gmi-alphame-cm
6	7	7	4	all	gmi-alphame-cm
7001	4	4	4	all	gmi-alphame-cm
8	7	7	4	all	gmi-alphame-cm
9	7	7	4	all	gmi-alphame-cm
911	3	3	4	all	gmi-alphame-cm

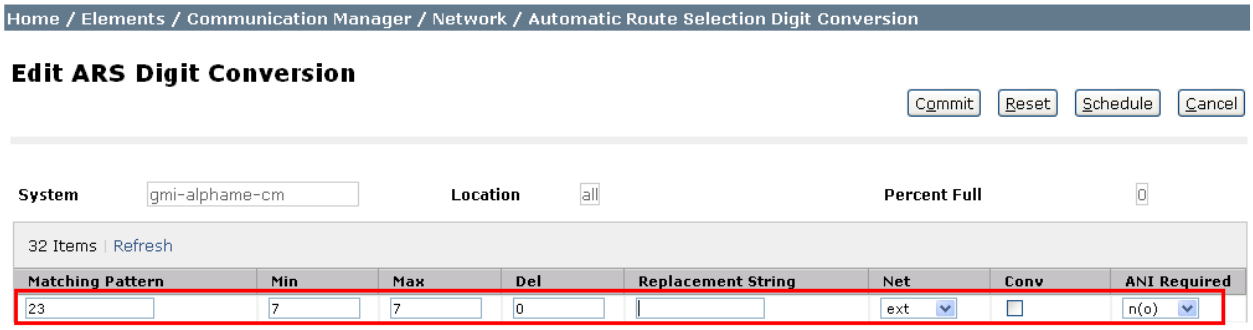
6.14. Administer ARS Digit Conversion

This section provides the configuration of the ARS Digit-Conversion rule used in the sample configuration for keeping inbound 7-digit calls local rather than routing back out to the Communication Server 1000. In order to support drag/drop calling from the Flare Communicator client contact fan (which is a 7-digit call) to other Converged Users, changes were made to the dial plan parameters form (see section 6.1). The changes made to the Dial Plan Parameters form routed 7-digit traffic to the **23x-xxxx** range off-net so that a 7-digit call will ring the Communication Server station first (invoking PCA/SIMRING capability) rather than just the Collaboration Client that is being called. Without a rule to keep inbound 7-digit traffic local, PCA calls to 7-digit SIP clients would also be routed off-net creating a loop condition. Inbound 7-digit calls will be kept local by using an ARS Digit-Conversion rule that states the **23x-xxxx** range represents extensions. The Incoming-Call Handling rule created in section 6.7 is inserting the digit '9' which routes the call to ARS. Before ARS Analysis is invoked, ARS Digit-Conversion rules are applied.

Navigating to System Manager-Elements-Communication Manager-Network-Automatic Route Selection Digit Conversion:

- Matching Pattern 23 (leading digits of Collaboration clients)
- Min 7 (length of Collaboration client extension)
- Max 7 (length of Collaboration client extension)
- Del 0 (no changes made to digit string)
- Net ext (defining this range as 'ext' prevents loop)
- Conv blank (no other conversion should be applied to this digit string)

Screen capture is below:



7. Avaya Aura® Presence Services Configuration

This section provides the procedures to verify the configuration of Avaya Aura® Presence Services. Presence Services can support collaboration clients such as Avaya Flare Communicator on iPad and Avaya one-X Mobile SIP for iOS client registered as SIP endpoints to Avaya Aura® Session Manager, as well as telephony clients such as M3900 / 1100 / 1200 series phones on the Communication Server 1000.

These instructions assume Presence Services has been installed and configured as described by **References [10]** through **[11]** in **Section 12.** For example, the configuration describing how Presence Services connects to several other elements in the network such as System Manager and Session Manager should be completed during installation. Therefore, this section will focus on verifying the configuration is correct.

Presence Services is configured using the browser-based **XCP Controller** graphical user interface. Access the **XCP Controller** interface using the URL "**https://<ip-address>:7300/admin**", where "**<ip-address>**" is the IP address of the server running Avaya Aura® Presence Services software. Log-in with the appropriate credentials.

7.1. Verify Configuration of Trusted Hosts

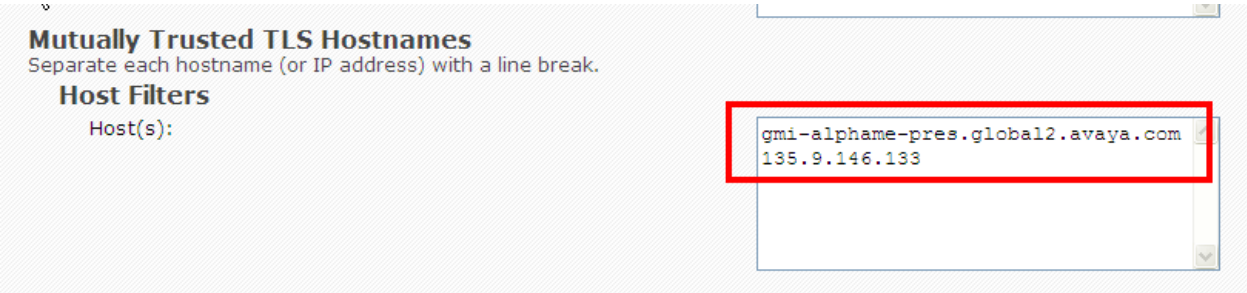
Step 1: Select "**Advanced**" from the drop-down menu for the **Configuration view:** field on the top right hand corner to enter the Advanced configuration mode.

In the **Router** section, select the **Edit** link associated with the **Plugin** component named "**Core Router**" as shown below.

Step 2: On the **Global Settings Configuration** page (not shown), scroll down to the **Mutually Trusted TLS Hostnames** section and verify the Fully Qualified Host Name of the server running Presence Services software has already been added in the **Host(s):** field.

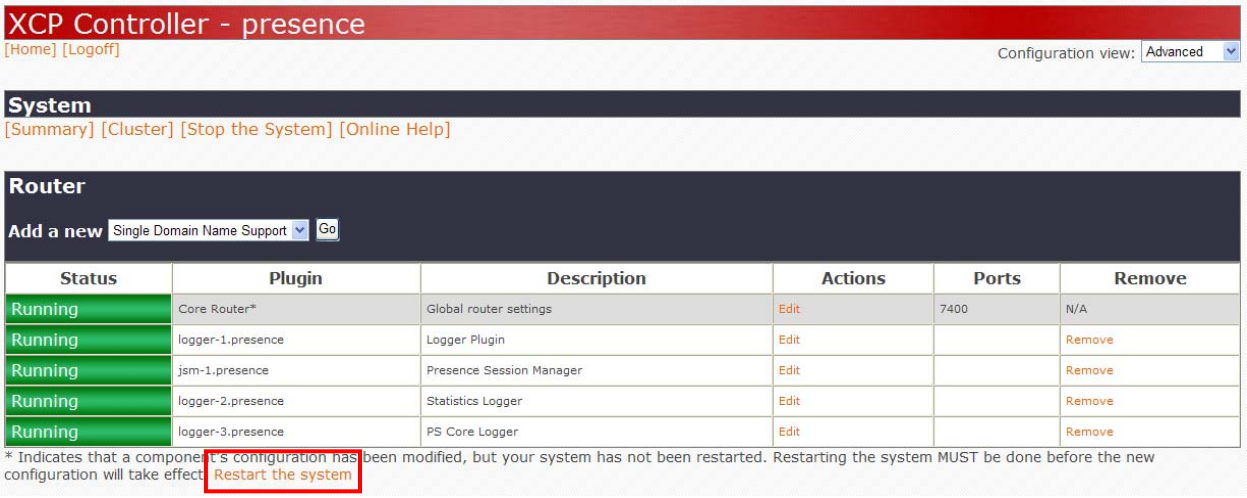
Verify IP addresses of SIP Signaling Interface of each Session Manager have also been entered in the same field.

For reference configuration, these values were "**gmi-alphame-pres.global2.avaya.com**", **135.9.146.133**"as shown below.

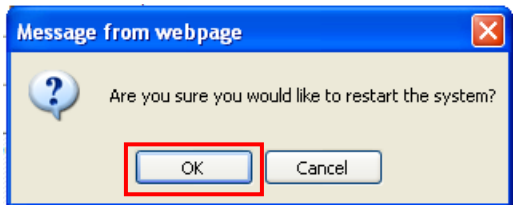


Click **Submit** to save changes.

Step 3: Select the **Restart the system** link for the changes to take effect.

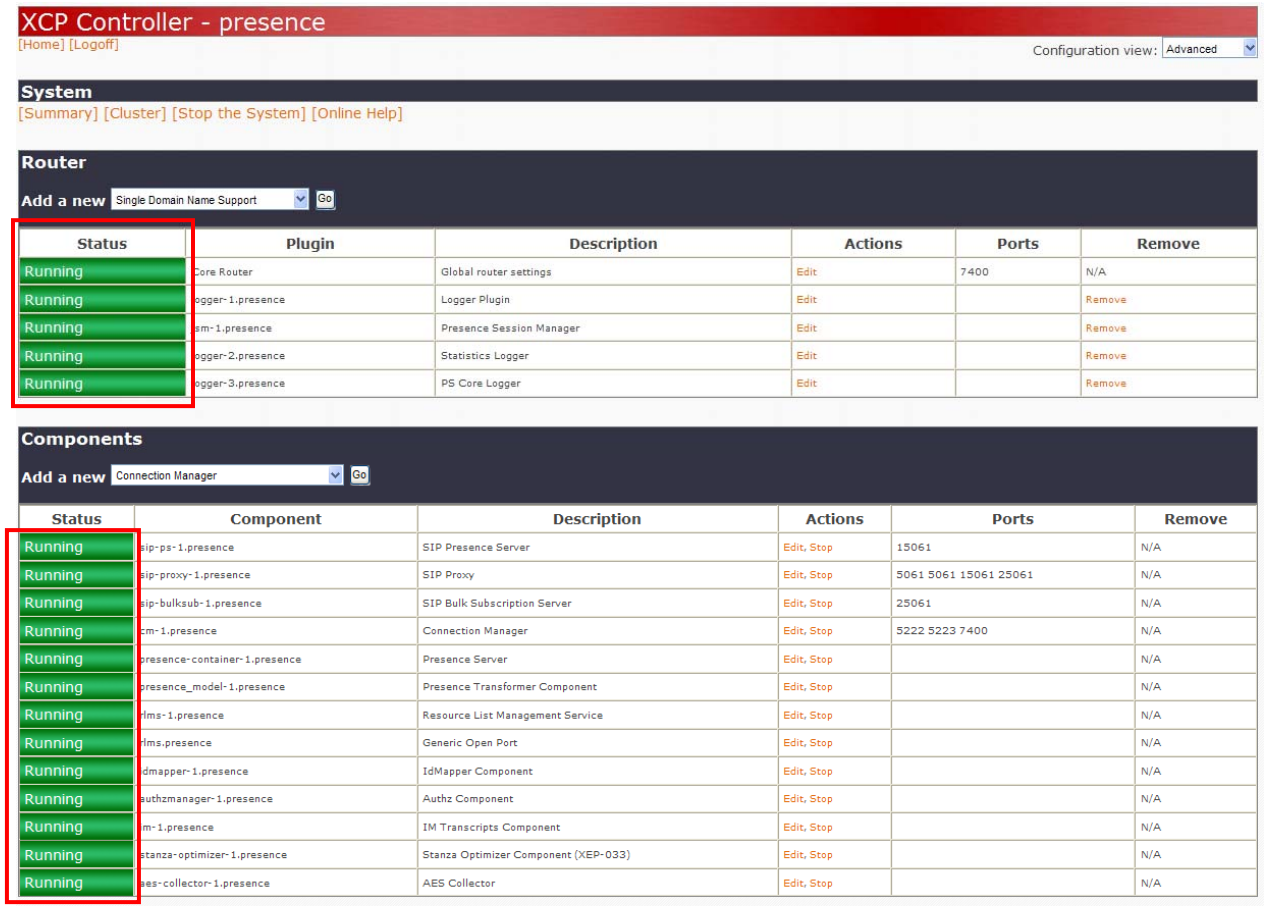


Click **OK** in the system dialog.



Step 4: Refresh the browser to verify the **Status** of all system components returns to "**Running**" as shown below:

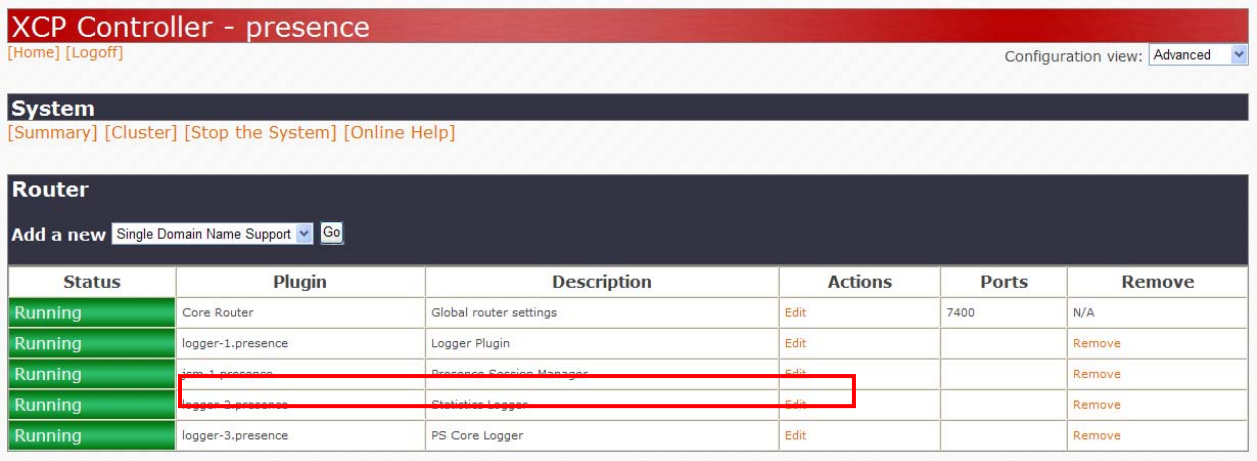
Note: the Restart operation may take several minutes to complete.



7.2. Verify Configuration to support Avaya SIP Endpoints

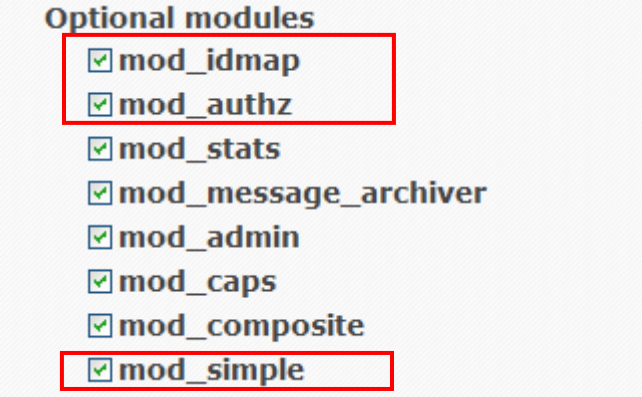
Step 1: Select "**Advanced**" from the drop-down menu for the **Configuration view:** field on the top right hand corner to enter the Advanced configuration mode.

In the **Router** section, select the **Edit** link associated the **Plugin** component named "**Presence Session Manager**" as shown below.



Step 2: On the **Presence Session Manager Configuration** page (not shown), scroll to the **Optional modules** section and verify the following modules have been selected as shown below.

- **mod_idmap** Verify ☑ has been entered.
- **mod_authz** Verify ☑ has been entered.
- **mod_simple** Verify ☑ has been entered.



Step 3: Scroll down to the **Module Configuration** section and verify the following fields have been configured:

- **SIP URI Mapping Configuration** Verify ☑ has been entered.
- **Send ID Mapping requests to an external component** Verify "**Yes**" has been selected.

Step 4: Click **Submit** (not shown) to save changes.

Step 5: Select the **Restart the system** link (not shown) as described in the **Section 5.1**.

8. Configure CallPilot

The assumption is that Callpilot is already installed and configured with voicemail boxes setup for the Communication Server 1000 clients. Please refer to **Reference [17] in Section 12** for detailed documentation.

The following is required:

- Verify CallPilot Service DN fits with the Collaboration Pack dial plan (not shown)
- Verify NMS is enabled (not shown)
- Registering CallPilot with System Manager
- Add CallPilot certificate to System Manager

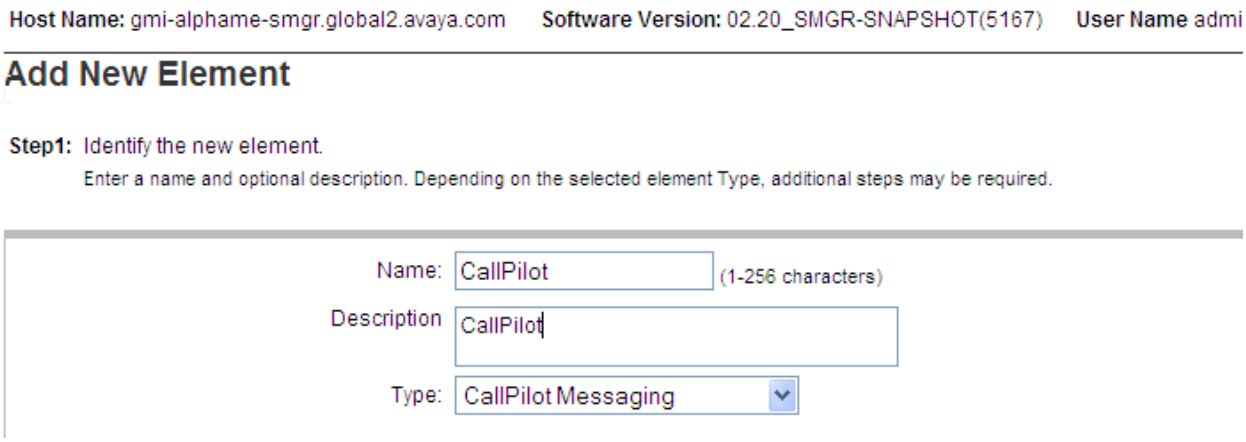
8.1. Registering CallPilot to the Element Registry

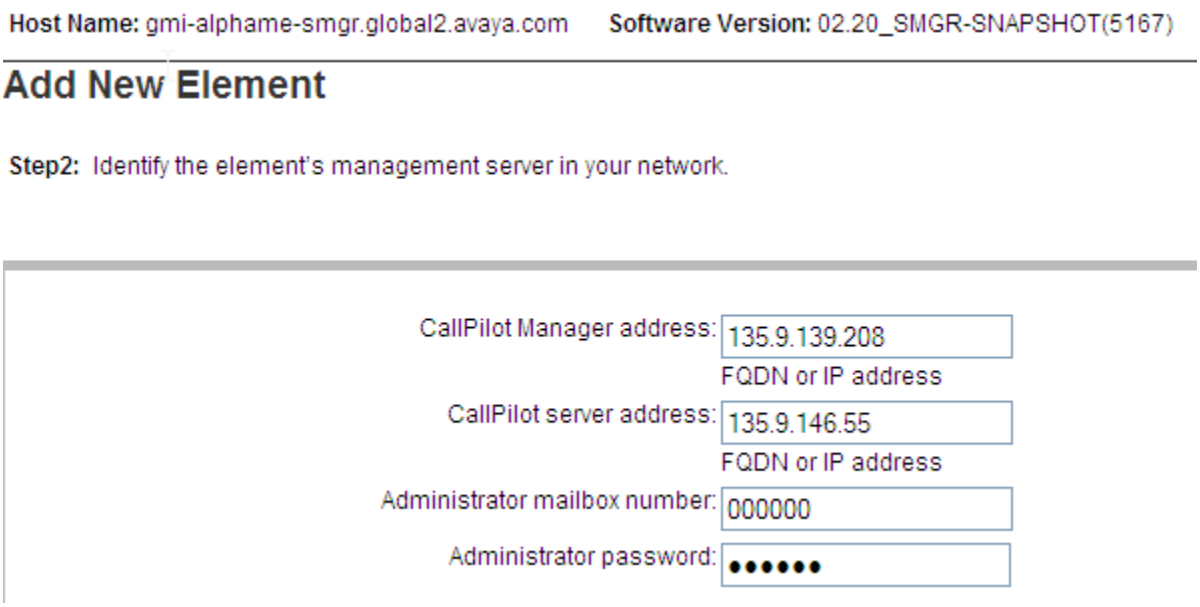
To be able to administer CallPilot via System Manager, CallPilot must be registered with System Manager.

Navigate to **UCM Services** – **Elements**- Select **Add**

• **Name**:	Specify the element name of the CallPilot, "**CallPilot**".
• **Description**:	Specify the element description of the CallPilot, "**CallPilot**"
• **Type**:	Select the element type from the drop-down list. On the Add New Element page, click **Next** and then specify the following:
• **CallPilot Manager address**:	Specify the FQDN or IP address of the CallPilot Manager,"**135.9.139.208**".
• **CallPilot server address**:	Specify the FQDN or IP address of the CallPilot server., "**135.9.146.55**".
• **Administrator mailbox number**:	Specify the administrator mailbox number. "**000000**"
• **Administrator password**:	Specify the administrator password. "**123456**"

Click **Save**.





8.2. Adding CallPilot certificate to System Manager

Navigate to **CallPilot Manager** secure URL and save the .cer file to desktop. For the reference configuration this is "**https:// 135.9.139.208/cpmgr**".

Navigate on the System Manager Web Console, to **Elements- Inventory** – Manage Elements

In the **Elements** section, select a managed element instance, "**System Manager 6.2**".

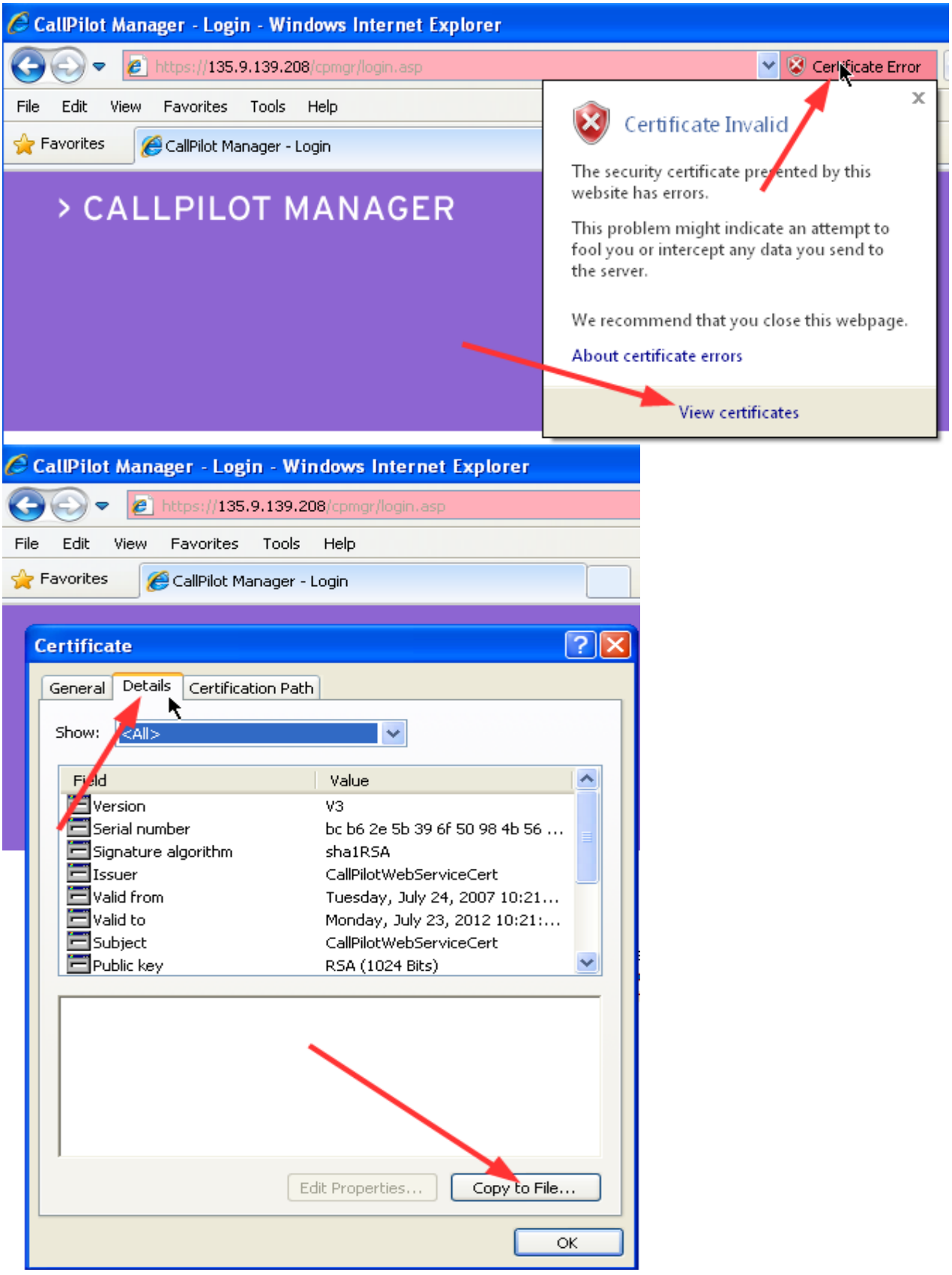
Select **More Actions - Configure Trusted Certificates**.

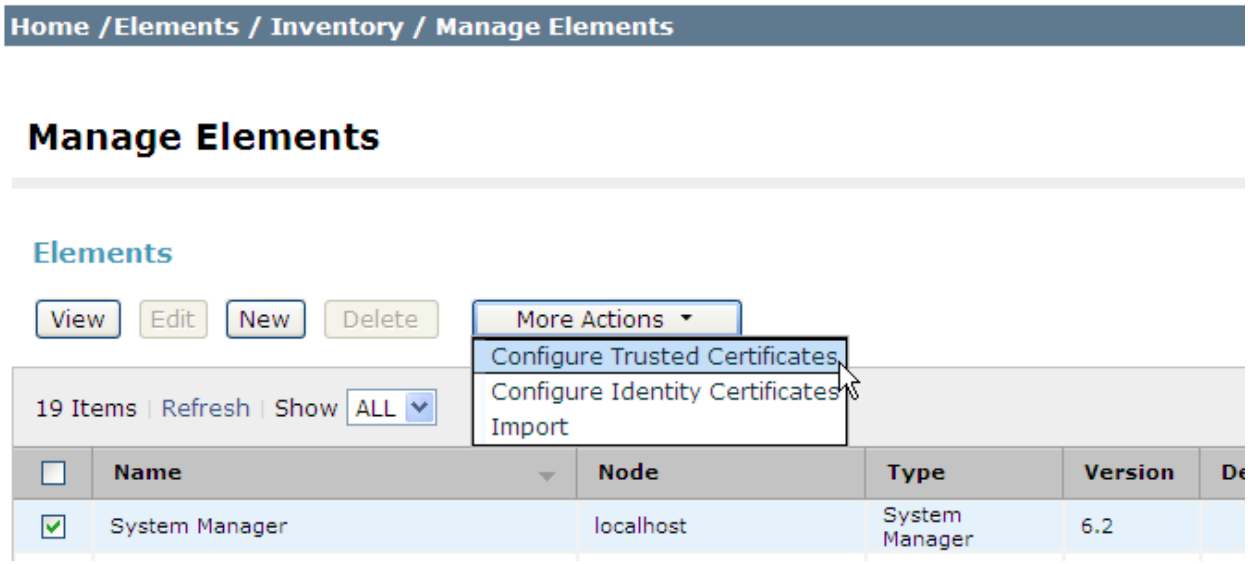
The system displays the certificates that are currently installed on the managed Element selected.

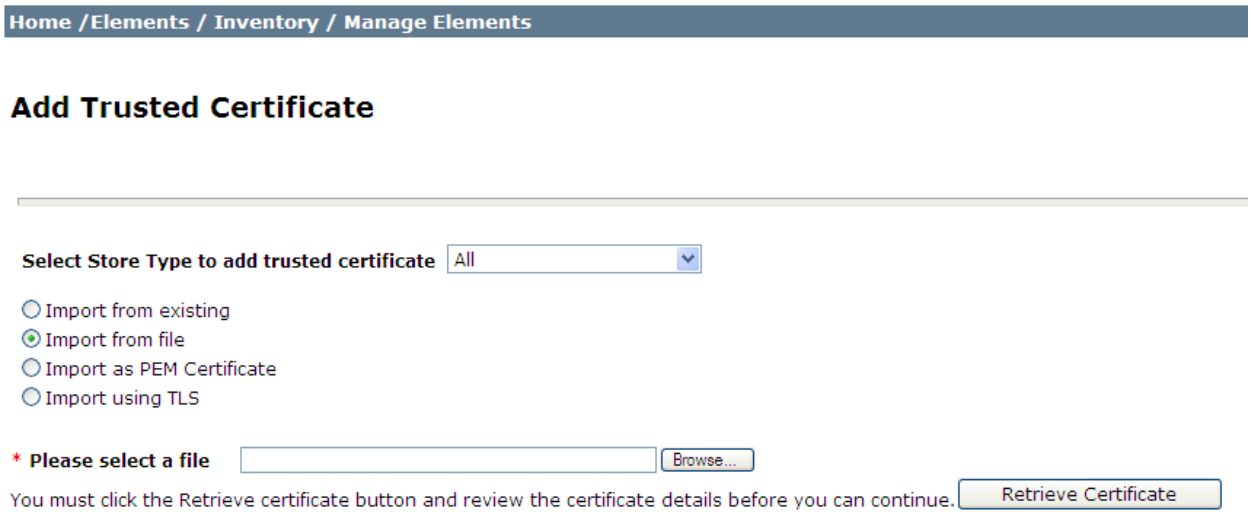
To add a CallPilot certificate, click **Add**. On the Add Trusted Certificate page, in the **Select Store Type to add trusted certificate** field, click **All**.

To add the certificate, Import the certificate by selecting "**Import from File**".

Click "**Commit**".







9. User Management

This section describes the details for configuring Converged Users across the Communication Server 1000 and the Collaboration Pack using Element Manager and System Manager User Management.

The Communication Address and Profile Extension number defined for Session Manager and Communication Manager will be a seven-digit number which is identical to corresponding Communication Server 1000 primary Directory Number and the route prefix. In the sample configuration, this would be "**23**52xx".

See **Reference [18]** in **Section 12** for more information on bulk importing and synchronizing of existing CS1000 users identities into System Manager.

The following assumes Midsize Enterprise template is configured as the Primary Security Server for the Unified Communications Management application and Communication Server 1000 is registered as a member of the System Manager Security framework.

The following administration steps will be described:

- Confirming users in Communication Server 1000 Element Manager
- Create User Identities and Communication profiles for Session Manager and Communication Manager
- Synchronize Communication Server 1000E Profile to User Identities in System Manager
- Synchronize CallPilot to User Identities in System Manager
- Create User Profile for Messaging (Call Pilot)
- Add PCA and Presence Services to Communication Server 1000E User Communication profiles

Note: Some administration screens have been abbreviated for clarity.

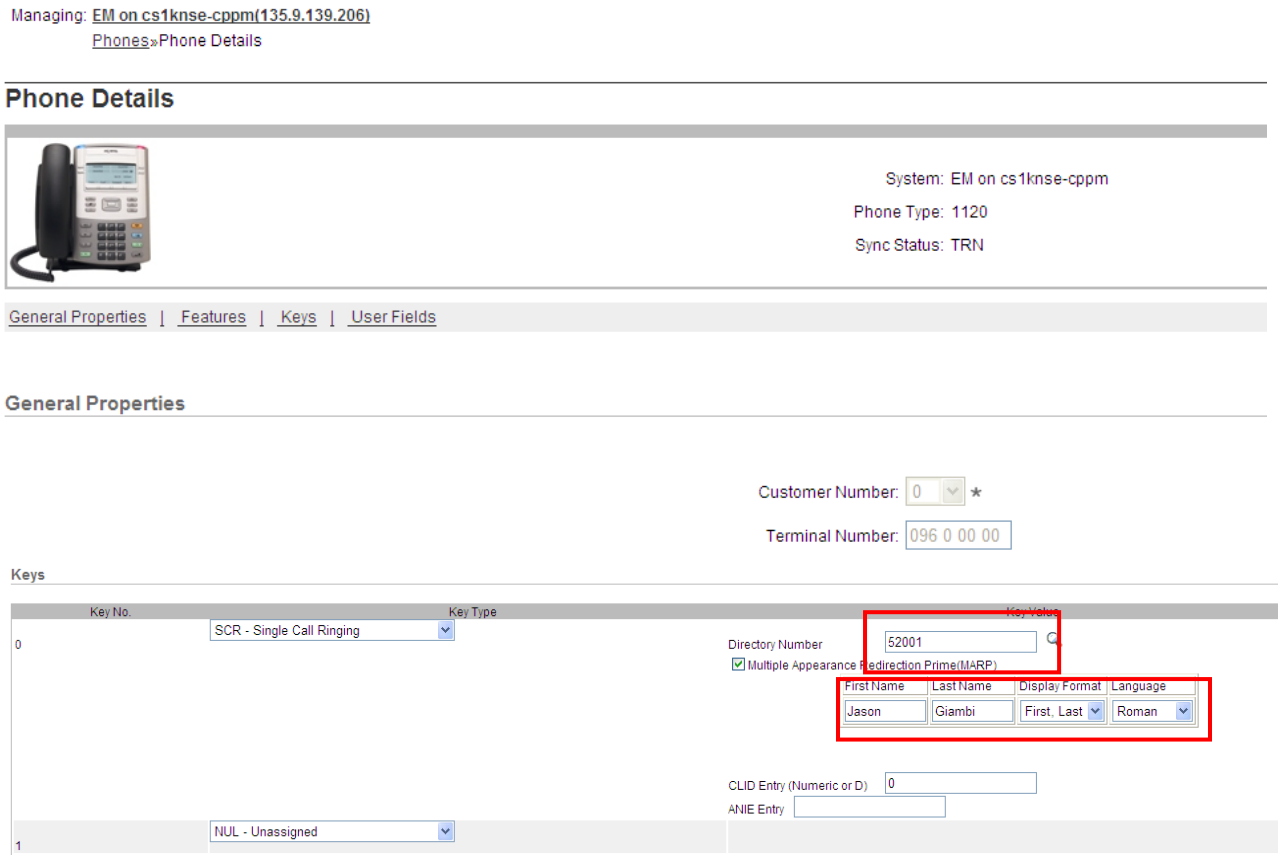
9.1. Create User Identities and Communication Profiles in System Manager

Communication Server 1000 users have been previously created on Communication Server 1000 Element Manager, with the main endpoint phone TN/DN and CPND (First Name Last Name).

For each Communication Server 1000 user defined in Element Manager a corresponding user identity must be added in System Manager. The **First Name** and **Last Name** of the user must match exactly on both Communication Server 1000 Element Manager and System Manager User Management. This is important for proper Presence synchronization as well as import synchronization for users of their Communication Server 1000 and CallPilot endpoint profile.

Access the web based GUI of Avaya Aura® System Manager by using the URL **"http://<ip-address>/SMGR"**, where **<ip-address>** is the IP address of Avaya Aura® System Manager. Login with the appropriate credentials.
Navigate to **UCM Services - Element Manager – Phone**

Example of a user defined in Element Manager for the sample configuration. Make note of the **First Name** and **Last Name** of the user.



There are several options for creating user identities in the User Profile Manager (UPM) of System Manager. See **Reference [18] in Section 12** for further information. For the sample configuration, users were manually created in UPM.

To create new users, on the web console for System Manager select **User Management** and then **Manage Users** from left navigation menu.

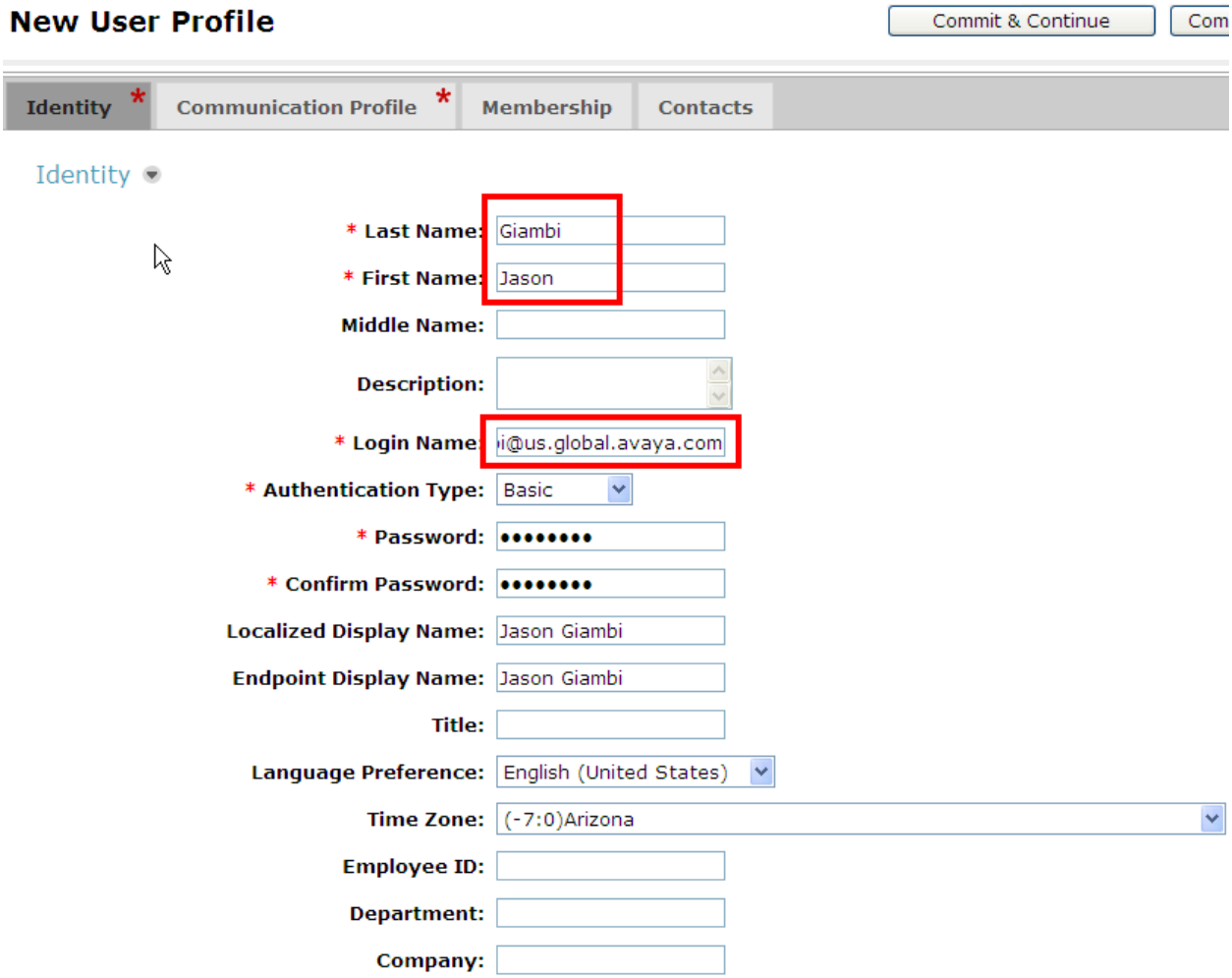
Click **New** (not shown). Enter values for the following required attributes for a new user in the Identity section and use default values for remaining fields.

- **Last Name:** Enter last name of user.

- **First Name:** Enter first name of user.
- **Login Name:** Enter "**handle"@<domain>**" where "**<domain>**" matches the domain defined in **Section 5.1**.
- **Authentication Type:** Verify "**Basic**" is selected.
- **Password:** Enter password used to log into System Manager.
- **Confirm Password:** Repeat value entered above.
- **Localized Display Name:** Enter display name for user [Optional].

The screen below shows results from for a new user.
The field names marked with an asterisk (*) are mandatory fields. Before you click **Commit & Continue** ensure that all the mandatory fields have valid information.

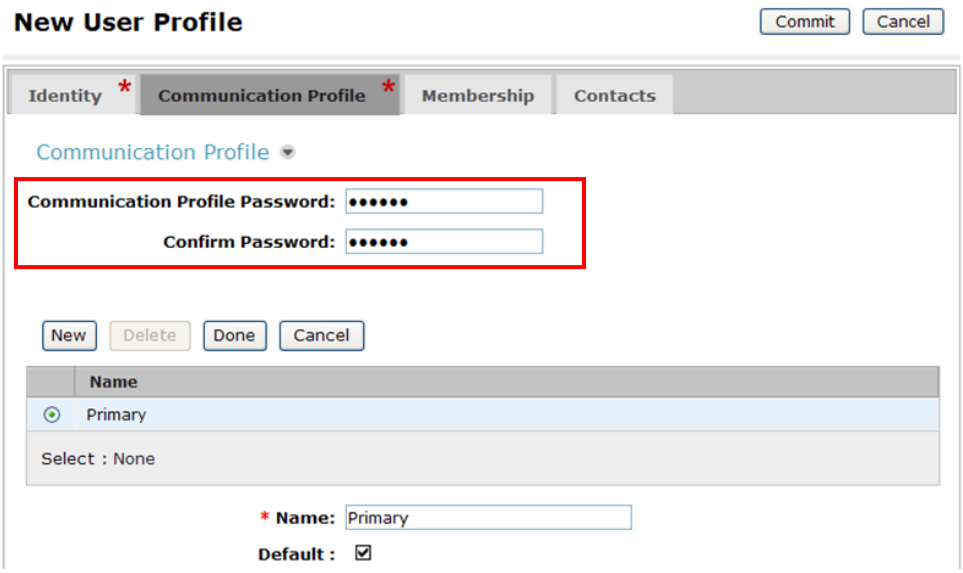
Using the reference configuration, user **Jason Giambi** is created.



Next select the **Communication Profile** tab and enter the value the user will use to register to Session Manager in the **Communication Profile Password** and **Confirm Password** fields.

Example: In the reference configuration, **"2352001"** is used as the password.

Verify there is a default entry identified as the **Primary** profile as shown below:



Next**,** Expand the **Communication Address** sub-section and select **New** to define a **Communication Address** for the new user. Enter values for the following required attributes:

- **Type:** Select "**Avaya SIP**" from drop-down menu.
- **Fully Qualified Address:** Enter same extension number as used for **Login Name** in **Step 1**.

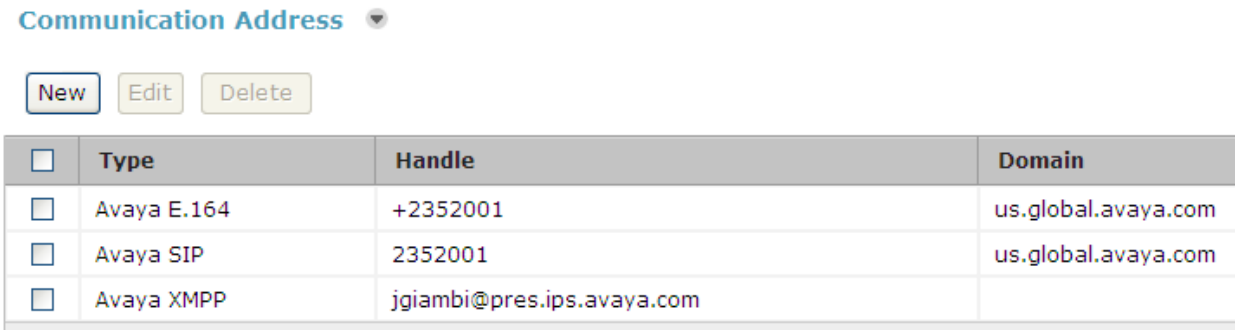
Note: value is shown in **Handle** field after address is added.

- **Domain:** Verify value matches Domain name defined in **Section 4.1**.

Repeat for the following to add Communication Address types **Avaya E.164.**

Note: The Avaya XMPP communication address is added automatically to the communication profile because Presence Services is enabled as part of the Avaya Midsize Enterprise template.

Click **Add** (not shown) to save the Communication Address. The screen below shows the results.

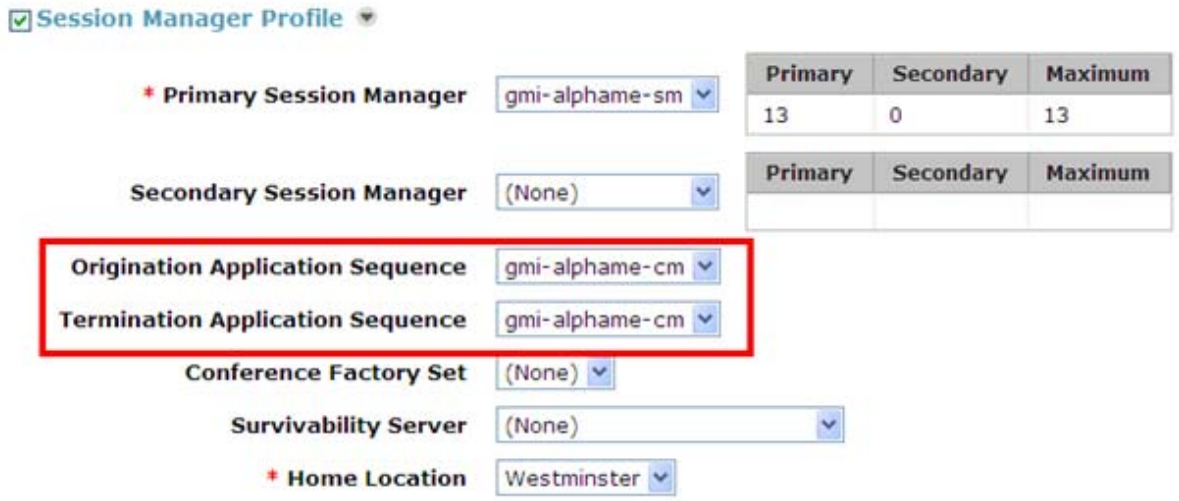


Scroll down to the **Session Manager Profile** section and enter ☑ to expand section.

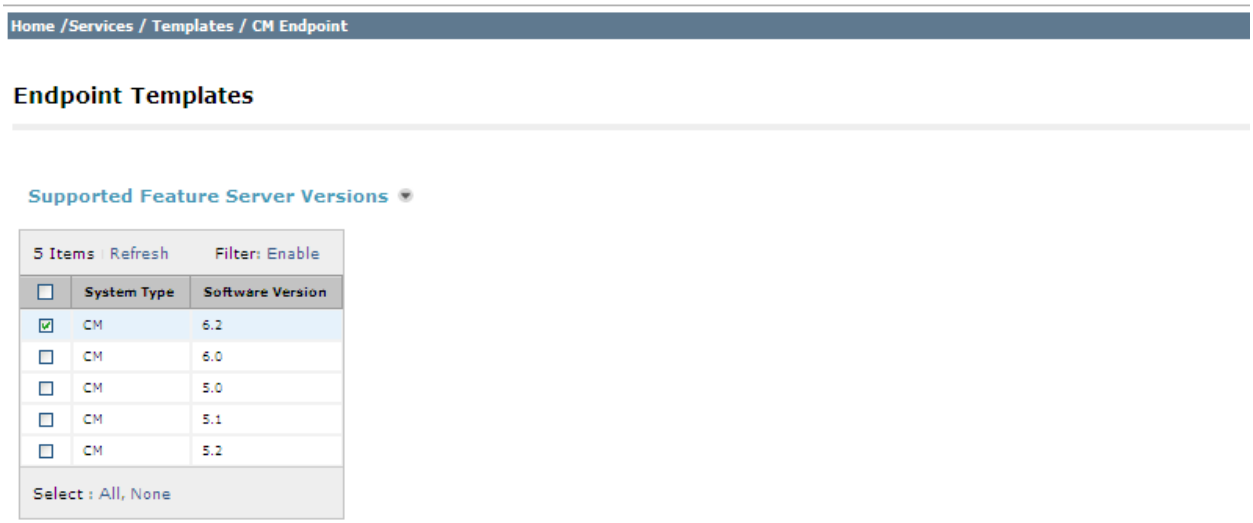
Enter the following values.

- **Primary Session Manager** — Select one of the Session Managers.
- **Origination Application Sequence** — Select **Application Sequence** defined for the Communication Manager (drop down available based on ME configuration).
- **Termination Application Sequence** — Select **Application Sequence** defined for the Communication Manager drop down available based on ME configuration).
- **Conference Factory Set** — Retain the default value of "**(None)**".
- **Survivability Server** — Select "**(None)**" from drop-down menu.
- **Home Location** — Select **Location**

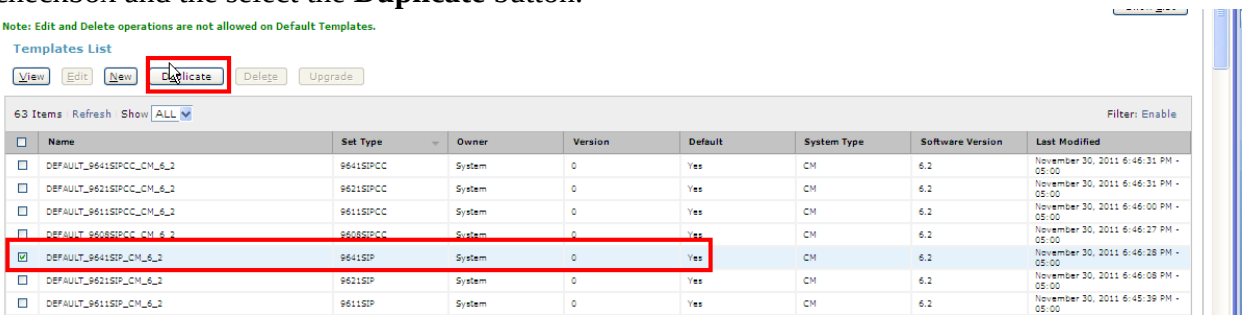
The screen below shows the results.



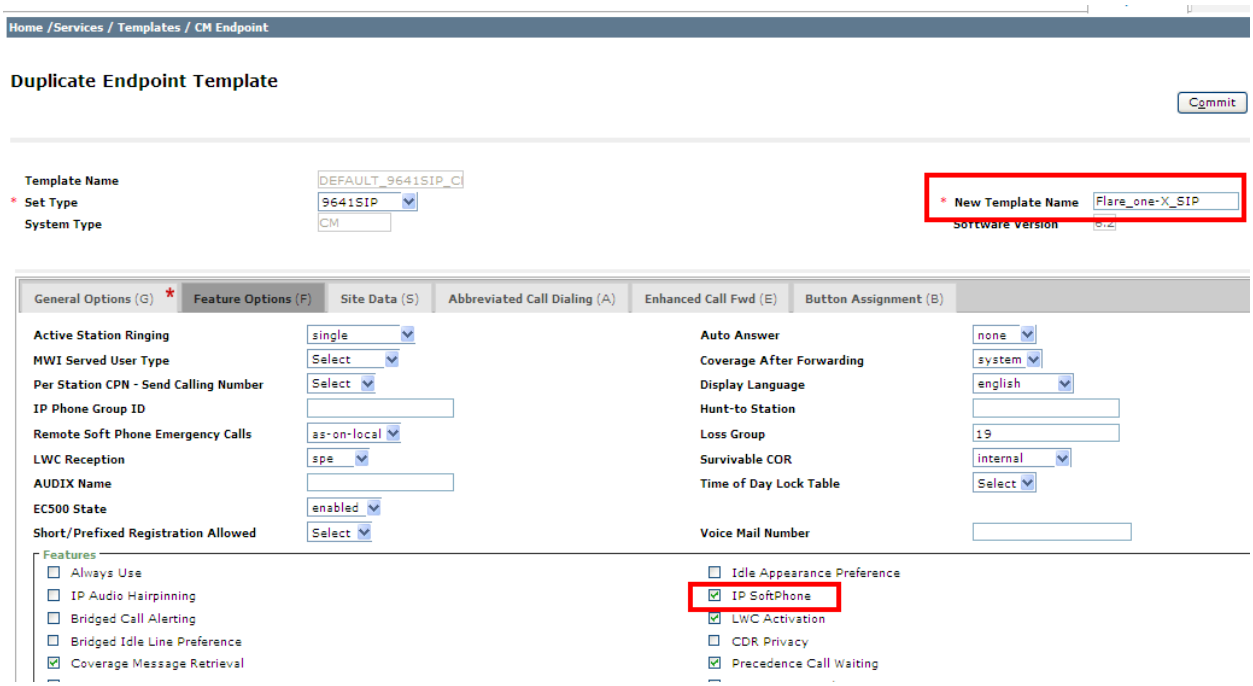
Prior to creating the Communication Manager endpoint profile for each user a customized template is recommended to be created. There is no standard template for Flare Communicator or one-X Mobile based collaboration clients. Using the default 9641 SIP template a duplicate may be made which can then be used for creating the Communication Manager endpoint profiles.
Navigate to **Services – Templates – CM Endpoint.** In the **Endpoint Templates** check the box for **System Type** and **Software Version** as **CM 6.2**.



In the following screen find the template, "**DEFAULT_9641SIP_CM_6_2**" and select the checkbox and the select the **Duplicate** button.



In the next screen, **Duplicate Endpoint Template**, enter in a name for the **New Template Name**, for the reference configuration, "**Flare_one-X_SIP**". Proceed to only check the box for "**IP Softphone**". Select **Commit** to save the new template.



Navigate back to **User Management** Users, and then for each user profile:

Scroll down to the **CM Endpoint Profile** section and enter ☑ to expand section.

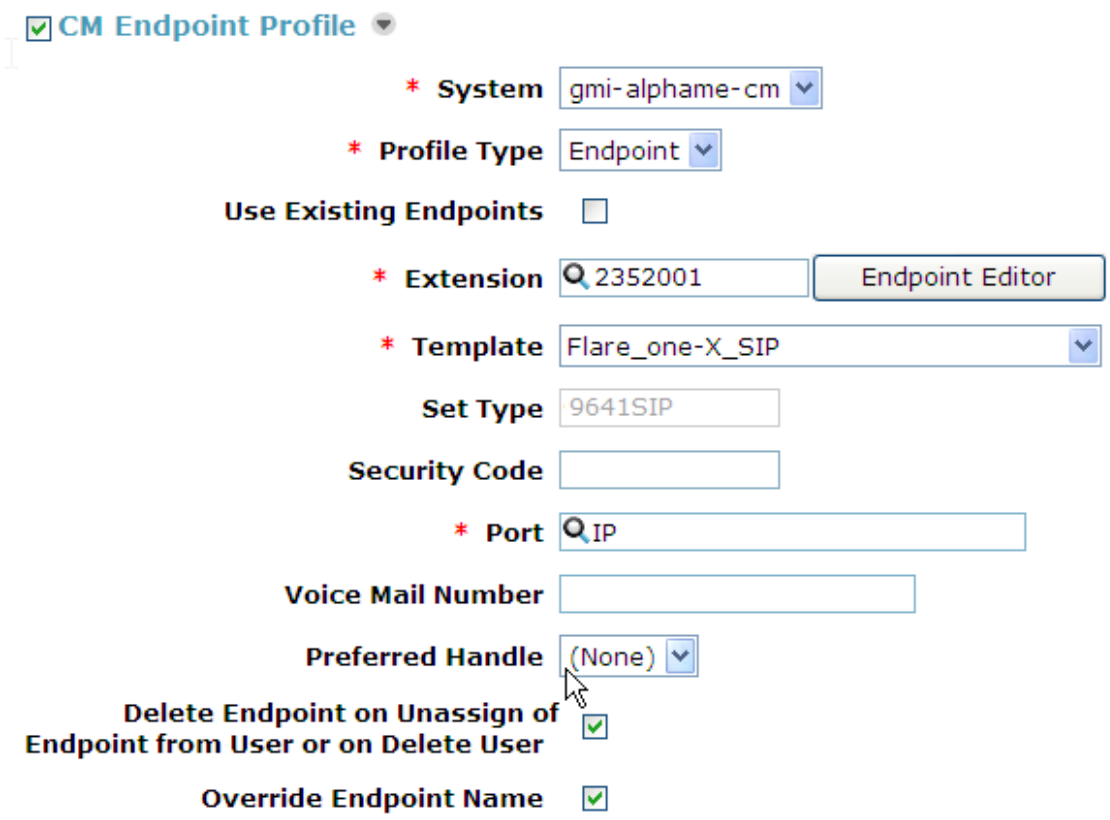
Enter the following values and use defaults for remaining fields.

- **System** Select Managed Element defined for Communication Manager
- **Profile Type** Select "**Endpoint**".
- **Use Existing Endpoints** Leave unchecked to automatically create new endpoint when a new user is created.
- **Extension** Enter same extension number used for **Login Name** in **Step 1**.
- **Template** Select the template named "**Flare_one-X_SIP**"
- **Security Code** Enter numeric value used to register the SIP endpoint.

Note: this field should match the value entered for the **Communication Profile Password** above, example "**2352001**"

- **Port** Select "**IP**" from drop down menu.
- **Voice Mail Number** Leave field blank.
- **Delete Station on Unassign of Endpoint** Enter ☑ to automatically delete station when **Endpoint Profile** is un-assigned from user [Optional].

The screen below shows the results from above when adding a new SIP user in the reference configuration.



Select the **Commit & Continue** button (not shown).

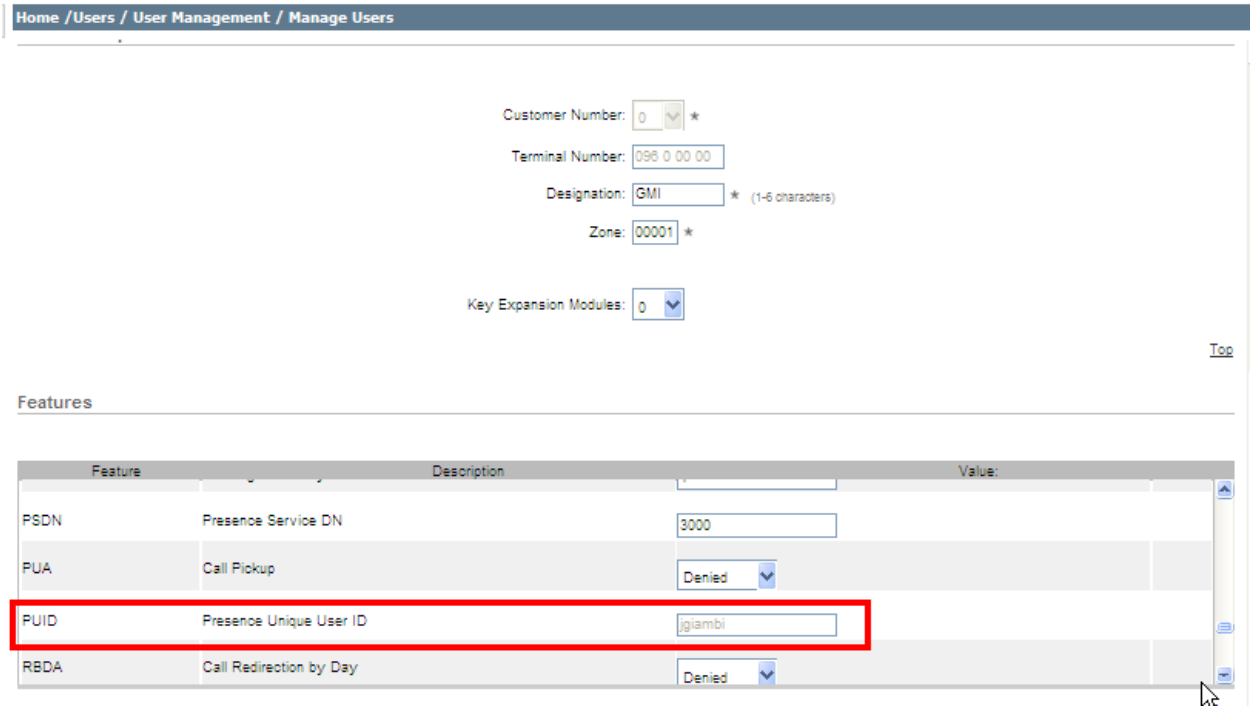
9.2. Synchronize Communication Profiles

System Manager provides the account synchronization feature to synchronize profile between Communication Server 1000 and CallPilot communication profile and their elements. Using this feature one can synchronize profiles in User Management with the profiles in the respective elements. During synchronization, the account synchronization feature uses the account data in the elements as the master data. Therefore, when a profile data is not in synchronization with the element, the account data from the element is copied to System Manager.

9.2.1. Communication Server 1000

This will import and synchronize all Communication Server 1000 users into their previously created System Manager Identity Communication Server 1000 Endpoint Profiles by matching each user (by **Firstname and Lastname)**.

Note: A key part of this synchronization is to populate the PSID into each CS1000 user's phone in Element Manager. For the reference configuration example, Jason Giambi, "**jgiambi**", see the screen capture below. The field is cannot be edited manually, only thru the following synchronization process.

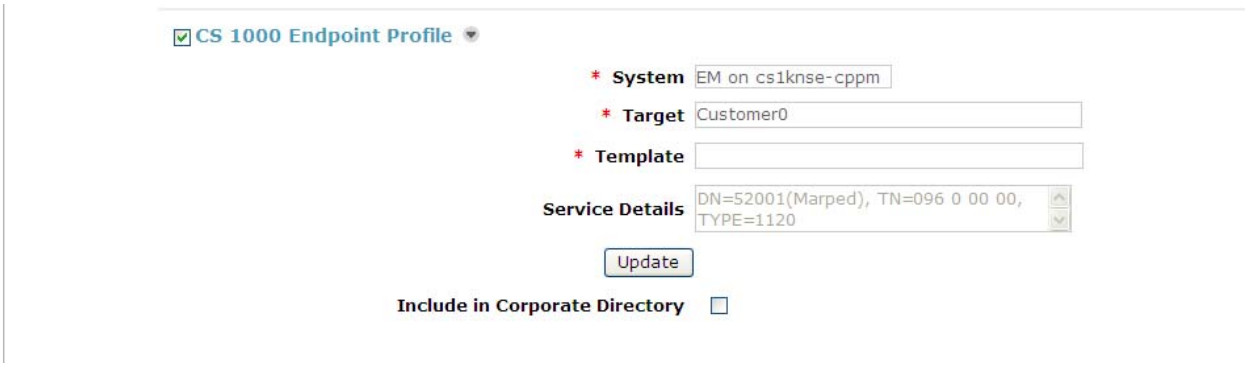


After building the user identities, perform an on demand synchronization. Navigate to **Elements → Inventory → Synchronization → Communication Server 1000 and CallPilot Synchronization.**

Select the row associated with the Communication Server 1000. Use the **Start** button to initiate the synchronization process. Use the **Refresh** button in the table header to verify status of the synchronization.

The above synchronization process will add the **CS 1000 Endpoint Profile** to System Manager for each user name match.

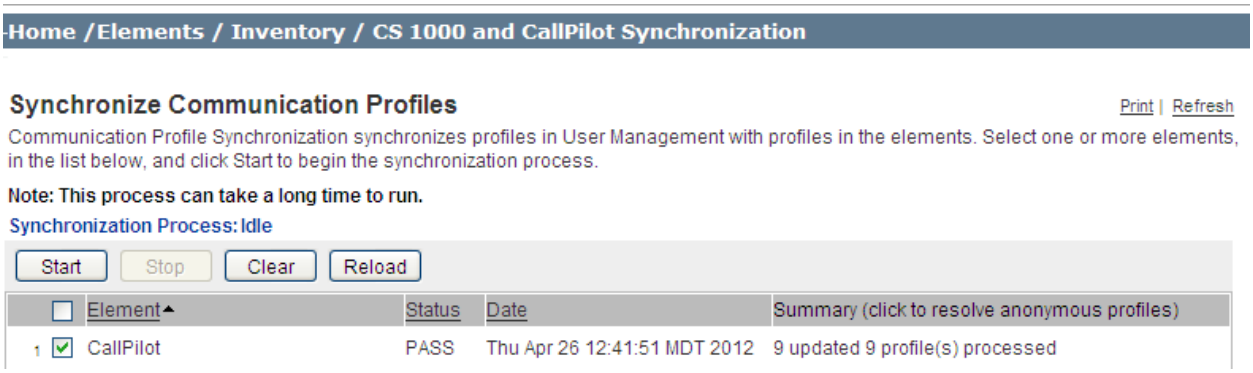
The following is the **CS 1000 Endpoint Profile** for an example for the reference configuration.



9.2.2. CallPilot

Next, perform an on demand synchronization to import CallPilot endpoint data to System Manager based on matching user identity data in UPM. Navigate to **Elements → Inventory → Synchronization → Communication Server 1000 and CallPilot Synchronization.**

Select the row associated with the CallPilot. Use the **Start** button to initiate the synchronization process. Use the **Refresh** button in the table header to verify status of the synchronization.



The above synchronization process will add the **CallPilot Endpoint Profile** to System Manager for each user name match.

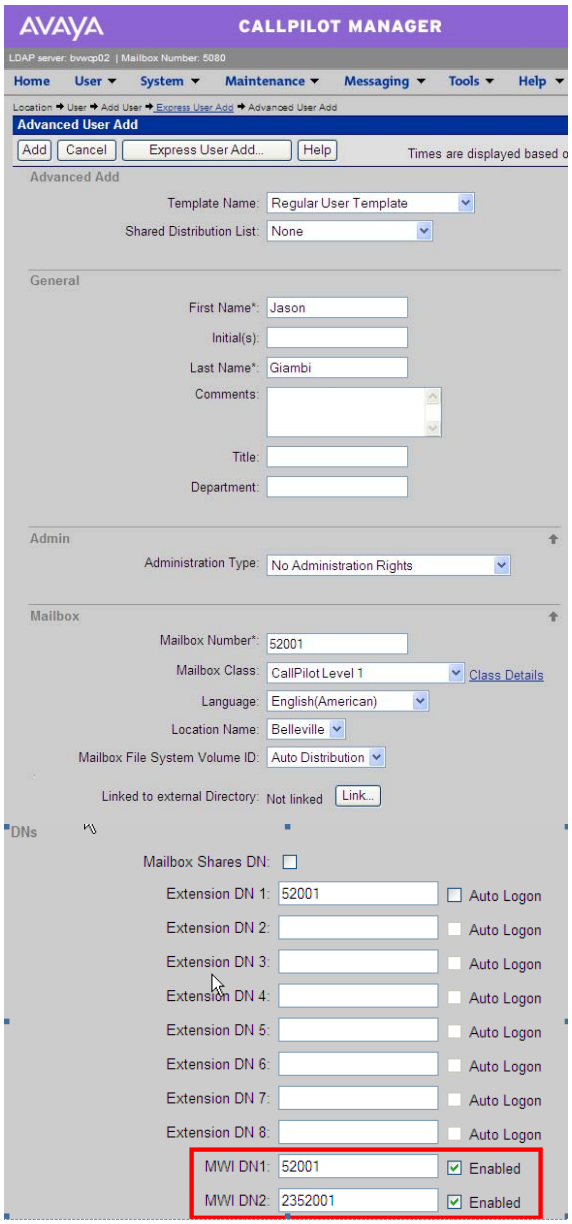
The following is the **CallPilot Endpoint Profile** for an example for the reference configuration.

9.3. Multiple Message Waiting Indication (MWI) for Collaboration

In support of the Converged User, specifically a single voicemail box, the existing CallPilot must be configured to send Message Waiting Indication (MWI) to the Avaya SIP endpoint. For the reference configuration this would be the one of the collaboration clients, one-X Mobile SIP for iOS as the Flare Communicator for iPad does not support MWI at this time.

Note: The assumption is the CallPilot mailboxes already exist for each Communication Server 1000 user. If not please refer to **Reference [17] in Section 12**.

To access CallPilot Manager please refer to the respect documentation as listed in the reference above. To enable the MWI for the twinned Avaya one-X Mobile SIP client enter in the **MWI DN #2** as "**2352xx**", as an example with the reference configuration this would be "**235200**1". The result is captured in the screen shot below. The user's twinned Communication Server 1000 client endpoint **MWI DN#1** is "**52001**"



9.4. Personal Call Assistant Configuration (PCA)

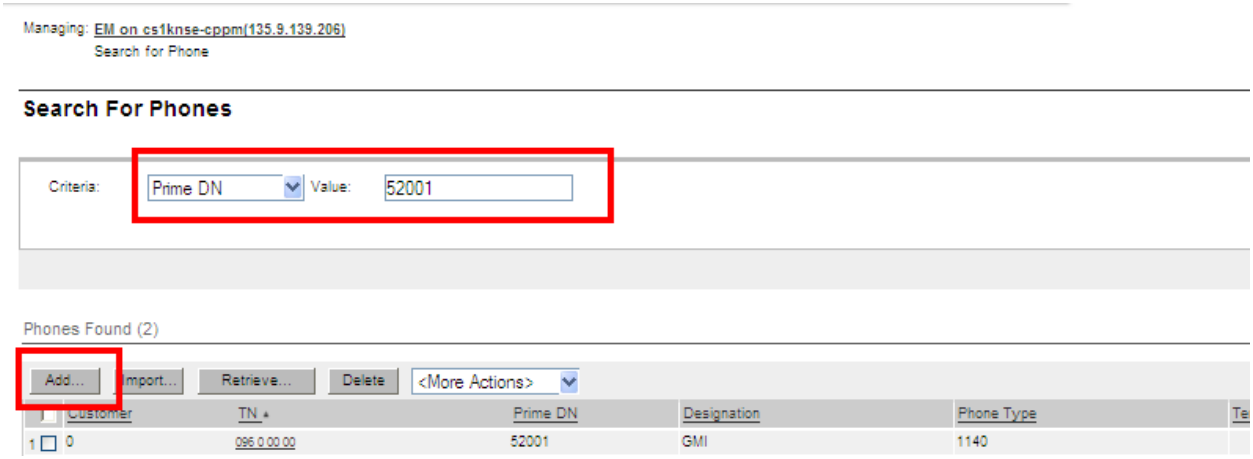
The PCA feature is utilized to enable the twinning of a Communication Server 1000 with an Avaya SIP endpoint (Avaya Aura® Flare Communicator or one-X Mobile Client) so that a "Converged User" may have simultaneous ringing, single number, single voicemail box and aggregated Presence.

To achieve the simultaneous ringing a corresponding PCA must be configured per Converged User. When the Communication Server client endpoint receives an incoming call, the PCA sends call signaling to the Avaya client endpoint via a Communication Server SIP trunk to the Session Manager to effectively "simultaneously ring" the Converged User's Avaya client endpoint.

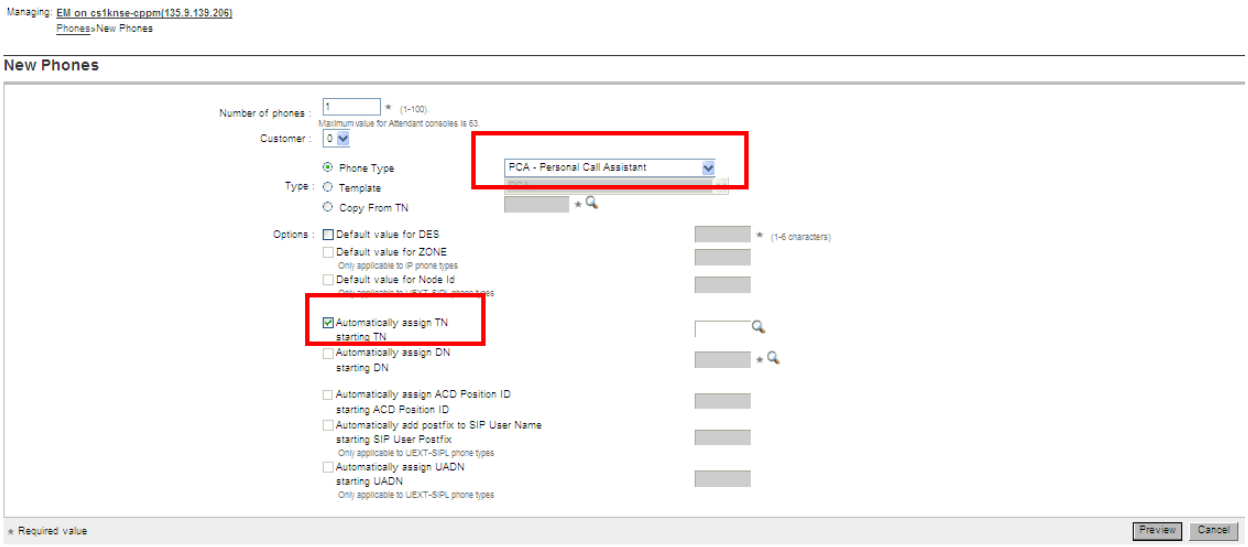
The following steps are required to enable this per user, refer to **Reference [6] in Section 12** for further details.

1. Ensure PCA is enabled in the Communication Server 1000 Customer Data Block (not shown).
2. Configure a PCA for every Communication Server 1000 phone user
    a. The PCA shares the same primary DN on key 0, as the Communication Server 1000 endpoint client.
    b. Configure key 0 as the Primary DN.
    c. Configure key 1 as HOT P key, with the AC2 target route prefix and DN as required to reach the twinned Avaya client endpoint.

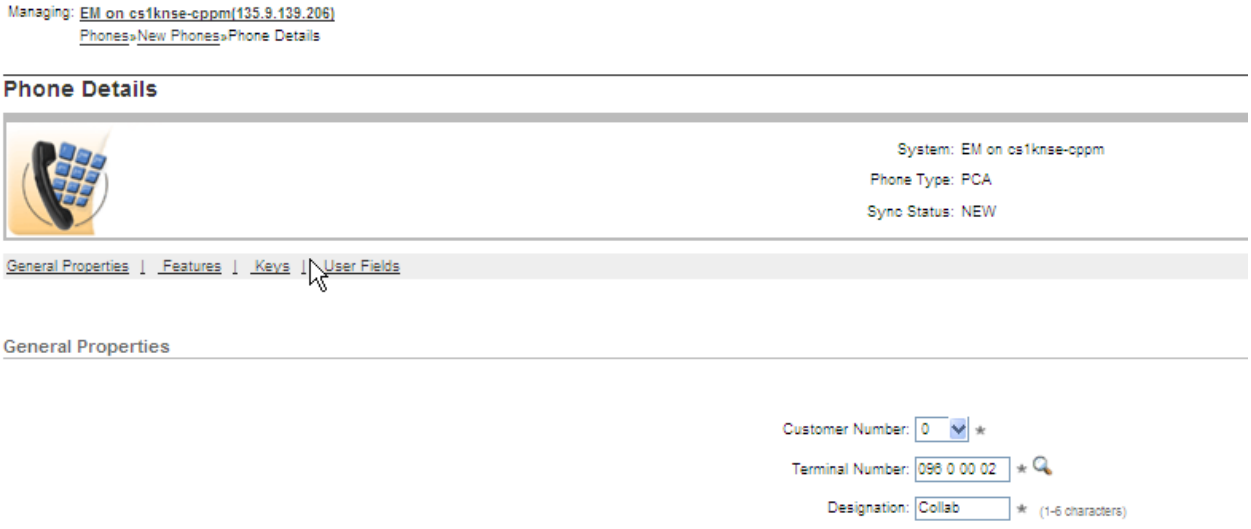
Navigate to **UCM – Element Manager – Phones**. Search for the **Prime DN** that a PCA is to be added to. For the reference configuration example "**52001**" was used. Next, select the **Add** button.



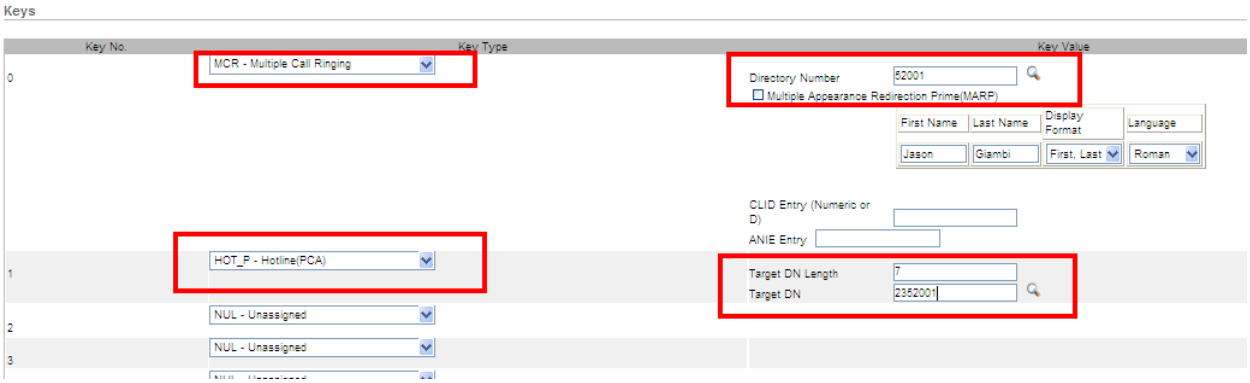
For **Phone Type** select **PCA-Personal Call Assistant** from the drop down menu. Next either enter in the TN or select box (as in this case) to **Automatically assign TN starting TN**. Select the **Preview** button.



The following screen will require input to **Customer Number** and **Designation**. For the reference configuration, **Customer Number** is "**0**" and **Designation** is "**Collab**".



On the same screen, under **Keys**, for **Key 0 select** "**MCR-Multiple Call Ringing**", for **Directory Number** enter "**52001**", **Key 1 select** "**Hot_P-Hotline (PCA)**". The **Target DN Length** is "**7**" and the **Target DN** is "**2352001**".



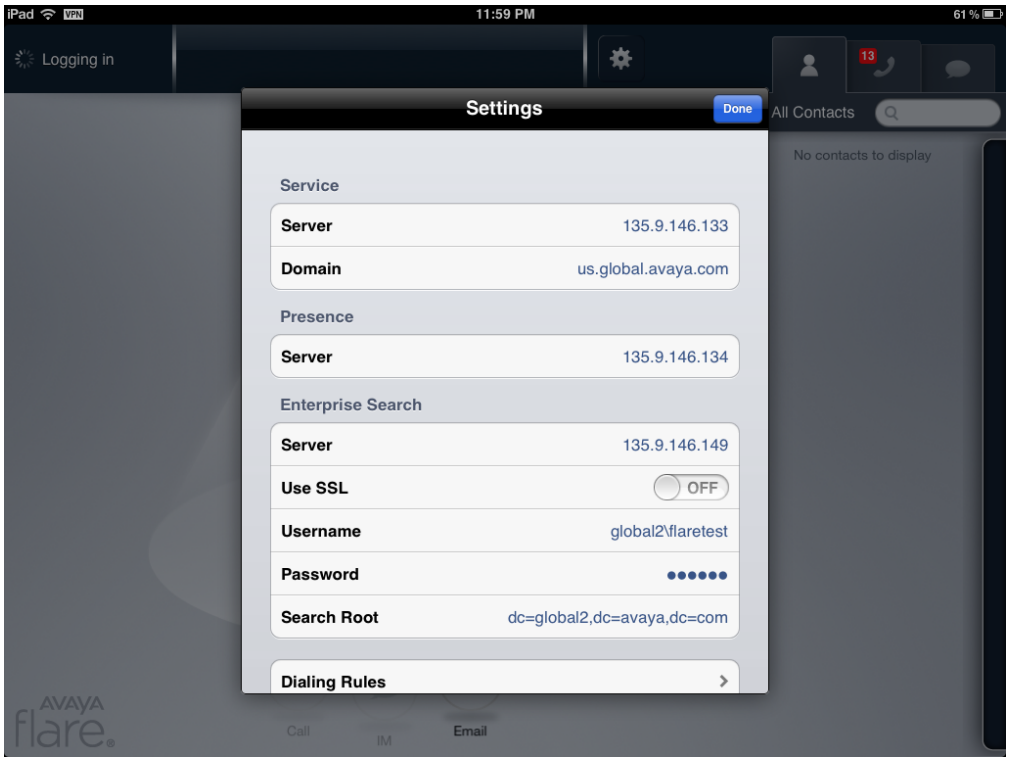
Select Commit (not shown) to save changes.

9.5. Manual Configuration of Avaya SIP Clients

This section defines the steps to manually configure Avaya Flare Communicator on iPad and Avaya one-X Mobile for SIP iOS running on iPhone/iPod to register to Session Manager.

9.5.1. Avaya Flare® Communicator on iPad

Refer to **Reference [19] to [21] in Section 12** on how to obtain, install and configure this client. For the reference configuration, **Server** is the Session Manager asset "**135.9.146.133**" and the Session Manager **Domain** "**us.global.avaya.com**". For **Presence Server** the IP address is "**135.9.146.134**".
For the reference configuration the setting for an external LDAP server for the **Enterprise Search Server** is "**135.9.146.149**". **SSL** is "**OFF**", **Username** "**global2\flaretest**", **Password** is "**password** "and **Search Root** is "**dc=global2,dc=avaya,dc=com**"

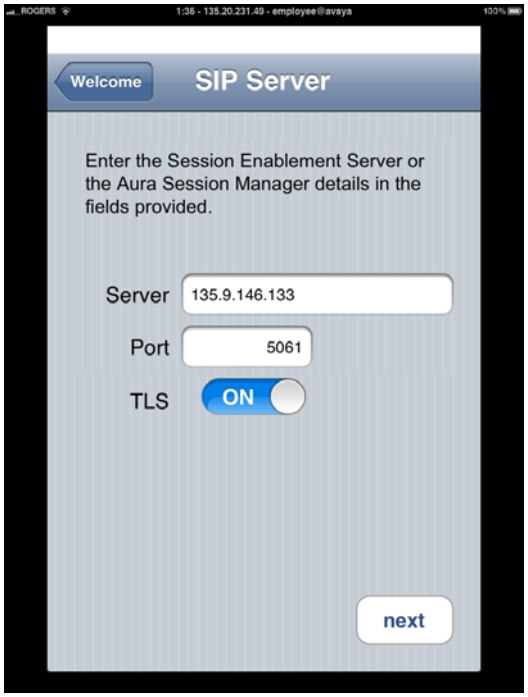


To login the user must provide the required login credentials, Extension and Password. As an example for the reference configuration, Extension is "**2352001**" and Password "**2352001**"

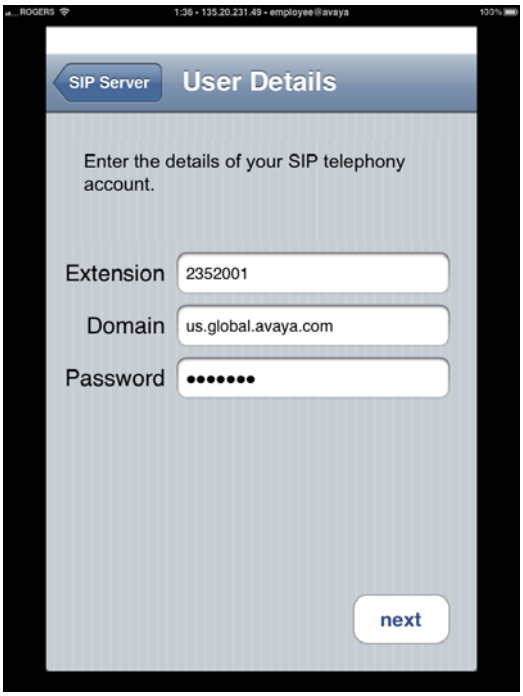
With the login step completed, the user is ready to make and receive calls, watch the Presence of buddies as well as IM with them.

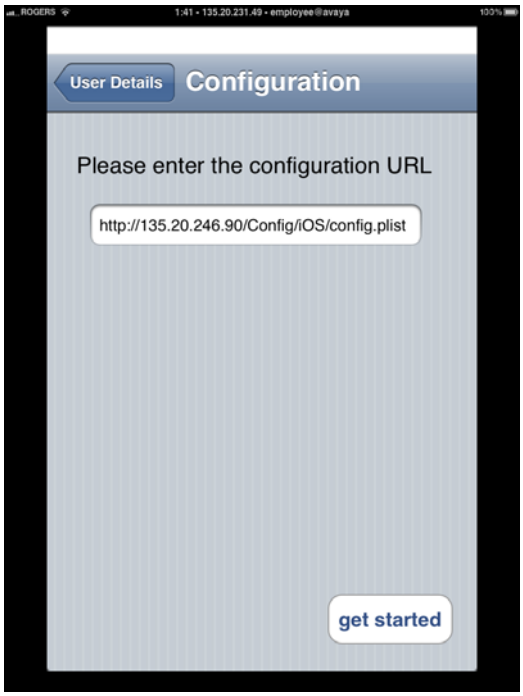
9.5.2. Avaya one-X Mobile SIP for iOS on iPhone

Refer to **Reference [22] and [23] in Section 12** on how to install and configure this client. For the reference configuration, **Server** is the Session Manager asset "**135.9.146.133**", **TLS** is "**On**". **Port** is "**5061**".

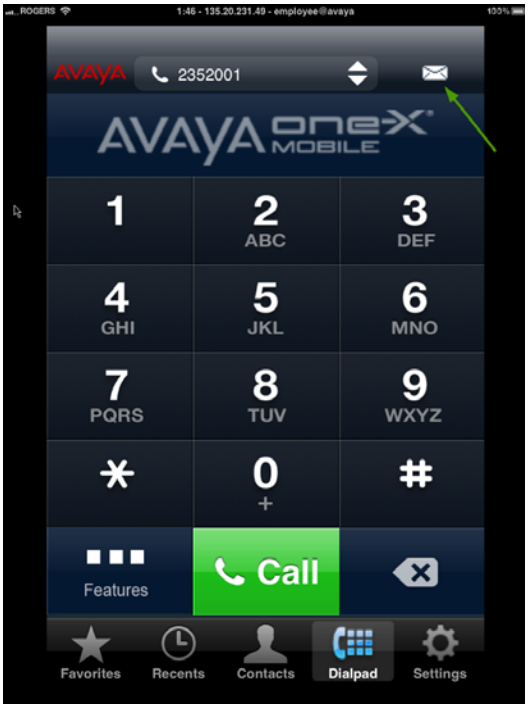


The **Extension** for this example reference configuration is "**2352001**" the Session Manager **Domain** "**us.global.avaya.com**". The **configuration URL** used was "**http:// 135.20.246.990/Config/iOS/config.plist**". Upon completion select the **get started** button.





The screen shot below is a capture of the example reference logged in and the mail icon (MWI) in the upper right hand corner indicating that there is a voicemail for this user.



10. Verification Steps

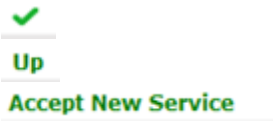
10.1. Verify Operational Status

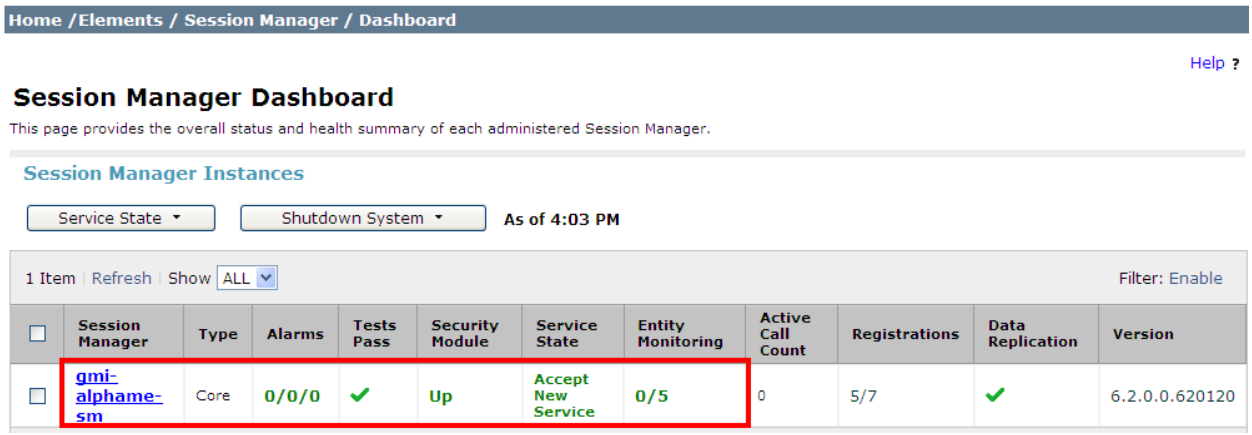
10.1.1. Verify Avaya Aura® Session Manager Operational Status

Navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager.

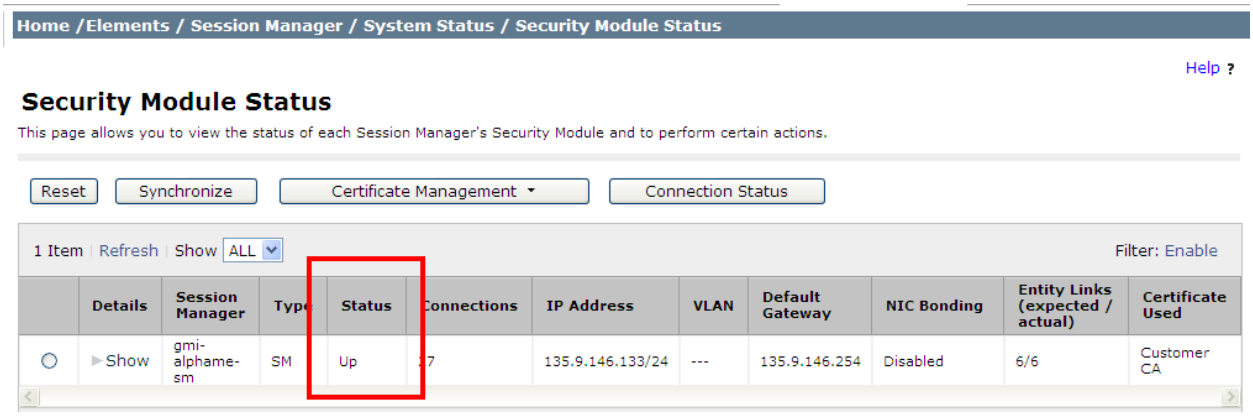
Specifically, verify the status of the following fields as shown below:

- **Tests Pass**
- **Security Module**
- **Service State**





Navigate to **Elements → Session Manager → System Status → Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays "**Up**" as shown below.

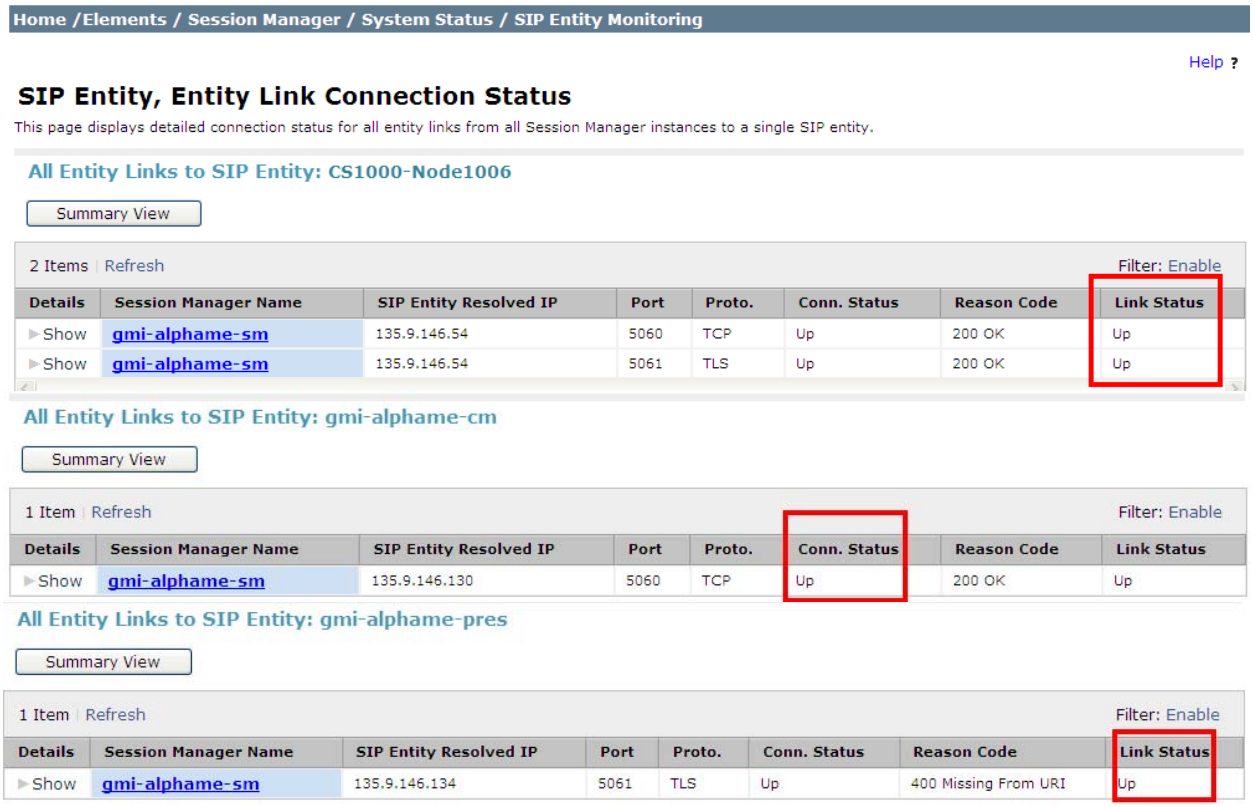


10.1.2. Verify SIP Entity Link Status

Navigate to **Elements - Session Manager - System Status - SIP Entity Monitoring** (not shown) to view more detailed status information for one of the SIP Entity Links.

Select the each SIP Entity from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page for each SIP entity.

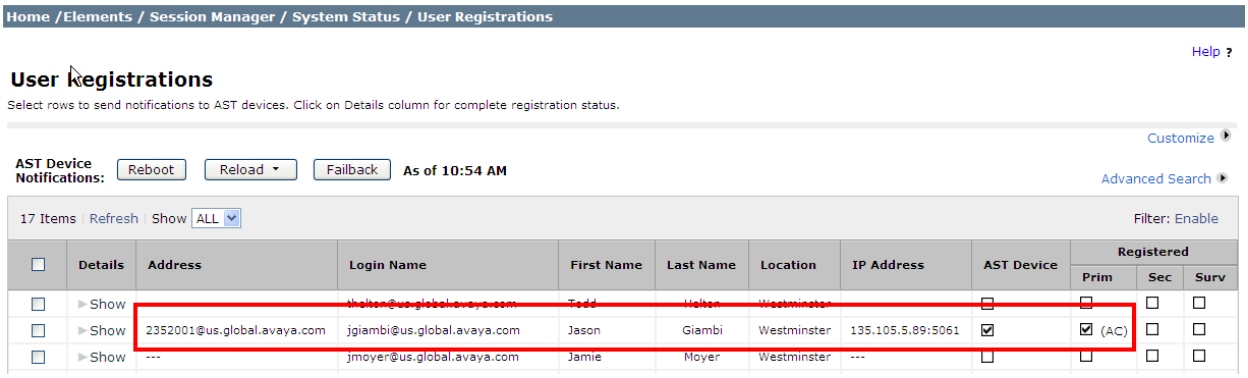
In each of the **All Entity Links to SIP Entity** table for each**: CS1000-Node 1006, gmi-alphame-cm and gmi-alphame-ps**, verify the **Conn. Status** for the link is "**Up**" as shown below.



10.1.3. Verify Registrations of SIP Endpoints

Navigate to **Elements - Session Manager - System Status - User Registrations** to verify the SIP endpoints have successfully registered with both Session Managers.

The screen below shows for the reference configuration the example user **Jason Giambi** is successfully registered with the Session Manager.



11. Conclusion

This Application Note describes the configuration and test results for the Collaboration Pack initial offer. The Collaboration Pack is made up of the Avaya Aura® Midsize Enterprise solution Release 6.2 and Avaya Communication Server 1000 Release 7.5. The solution enables a traditional Communication Server 1000 client to be twinned with a collaboration client such as the Flare Communicator for iPad and the one-X Mobile – this creates a "Converged User". This capability provides a Communication Server 1000 user to leverage Unified Collaboration capabilities of the Avaya Aura® Midsize Enterprise solution.

Further Application Notes will be published as additional capabilities are tested and documented with the "Collaboration Pack for CS 1000".

12. Additional References

The following documentation may be obtained from http://support.avaya.com.

1. ME Intelligent Workbook
2. Overview of Avaya Aura® Solution for Midsize Enterprise, Release 6.2, Issue 2.2, April 2012
3. Implementing AA solution for Midsize Enterprise Template Release 6.2, Issue 4, April 2012
4. Installation and Upgrades for the Avaya G430 Branch Gateway, Release 6.1, 03-603233, Issue 5, February 2012
5. Network Routing Service Fundamentals Avaya Communication Server 1000, Release 7.5, NN43001-130, 03.10, September 2011
6. IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313,
7. Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116,
8. Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125,
9. Administering Avaya Aura® Presence Services Release 6.1
10. Administering Avaya Aura® Presence Services XCP Controller
11. Implementing Avaya Aura® Presence Services Release 6.1
12. Presence Services with Communication Server 1000, Document Number NN43001-141, Dec 2011
13. Administering Avaya Aura® Communication Manager, Doc ID 03-300509.
14. Administering Avaya Aura® Communication Manager Server Options, Doc ID 03-603479.
15. Avaya Toll Fraud Security Guide, Doc ID 555-025-600.
16. Avaya Communication Server 1000 and Avaya CallPilot Server Configuration, Document Number NN42300-312
17. Administrating Avaya Aura® System Manager, Release 6.2, March 2012.
18. Avaya Flare Overview and Planning Issue 1
19. Administering Avaya Flare Communicator for iPad Devices
20. Implementing Avaya Flare Communicator for iPad Devices
21. Avaya one-X Mobile SIP iOS User Guide
22. Avaya one-X for Apple SIP Clients Administration Guide

13. Change History

Issue	Date	Reason
1.0	13/6/2012	Initial issue

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com